https://doi.org/10.15388/vu.thesis.785
https://orcid.org/0000-0002-3870-7330

VILNIUS UNIVERSITY

Arnoldas Budžys

Deep Learning-Based Keystroke Dynamics Authentication for Insider Threat Detection in Critical Infrastructure

DOCTORAL DISSERTATION

Natural Sciences,
Informatics (N 009)

VILNIUS 2025

The dissertation was prepared between 2020 and 2024 at Vilnius University.

Academic Supervisor – Assoc. Prof. Dr. Viktor Medvedev (Vilnius University, Natural Sciences, Informatics – N 009).

This doctoral dissertation will be defended in a public meeting of the Dissertation Defence Panel:

Chairman – Prof. Dr. Julius Žilinskas (Vilnius University, Natural Sciences, Informatics – N 009).
Members:
Dr. Gražina Korvel (Vilnius University, Natural Sciences, Informatics – N 009),
Prof. Dr. Jurgita Markevičiūtė (Vilnius University, Natural Sciences, Mathematics – N 001),
Prof. Dr. Audris Mockus (University of Tennessee, USA, Natural Sciences, Informatics – N 009),
Prof. Dr. Dmitrij Šešok (Vilnius Gediminas Technical University, Natural Sciences, Informatics – N 009).

The dissertation shall be defended at a public meeting of the Dissertation Defense Panel at 1:00 p.m. on 1st of July 2025 in room 203 of the Institute of Data Science and Digital Technologies of Vilnius University.
Address: Akademijos str. 4, LT-04812, Vilnius, Lithuania
Tel. +370 5 210 9300; e-mail: info@mii.vu.lt

The text of this dissertation can be accessed at the Library of Vilnius University, as well on the website of Vilnius University:
https://www.vu.lt/lt/naujienos/ivykiu-kalendorius.

https://doi.org/10.15388/vu.thesis.785
https://orcid.org/0000-0002-3870-7330

VILNIAUS UNIVERSITETAS

Arnoldas Budžys

Giliuoju mokymusi pagrįstas klavišų paspaudimų dinamikos autentifikavimas vidinių grėsmių aptikimui ypatingos svarbos infrastruktūroje

DAKTARO DISERTACIJA

Gamtos mokslai,
Informatika (N 009)

VILNIUS 2025

Disertacija rengta 2020–2024 metais Vilniaus universitete.

Mokslinis vadovas – doc. dr. Viktor Medvedev (Vilniaus universitetas, gamtos mokslai, informatika – N 009).

Gynimo taryba:
Pirmininkas – prof. dr. Julius Žilinskas (Vilniaus universitetas, gamtos mokslai, informatika – N 009).
Nariai:
dr. Gražina Korvel (Vilniaus universitetas, gamtos mokslai, informatika – N 009),
prof. dr. Jurgita Markevičiūtė (Vilniaus universitetas, gamtos mokslai, matematika – N 001),
prof. dr. Audris Mockus (Tenesio universitetas, JAV, gamtos mokslai, informatika – N 009),
prof. dr. Dmitrij Šešok (Vilniaus Gedimino technikos universitetas, gamtos mokslai, informatika – N 009).

Disertacija ginama viešame Gynimo tarybos posėdyje 2025 m. liepos 1 d. 13:00 val. Vilniaus universiteto Duomenų mokslo ir skaitmeninių technologijų instituto 203 auditorijoje. Adresas: Akademijos g. 4, LT-04812, Vilnius, Lietuva, tel. +370 5 210 9300; el. paštas: info@mii.vu.lt.

Disertaciją galima peržiūrėti Vilniaus universiteto bibliotekoje ir Vilniaus universiteto interneto svetainėje adresu: *https://www.vu.lt/lt/naujienos/ivykiu-kalendorius*.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Dr. Viktor Medvedev and prof. Dr. Olga Kurasova for their help and advice during the time of this thesis. I also appreciate the comments and suggestions provided by the reviewers Prof. Dr. Audris Mockus and Prof. Dr. Julius Žilinskas. I would like to thank the commanders of the Communications and Information Systems Battalion of the Grand Hetman Kristupas Radvila Perkūnas of the Lithuanian Armed Forces for granting me study holidays and the available time to complete my thesis. Finally, I am grateful to my family for their support and understanding.

ABSTRACT

Cybersecurity in critical infrastructure requires advanced authentication systems to effectively address the issues of unauthorized access and insider threats. This thesis proposes a novel approach based on the GAFMAT method, which transforms keystroke dynamics data into detailed image representations and thus significantly enhances the ability to distinguish human typing patterns. A Siamese neural network architecture, incorporating convolutional neural network branches, is utilized for the purpose of trustworthy user authentication, thereby enabling the effective distinction between legitimate and illegitimate access attempts. To enhance the accuracy of the authentication process and adapt the methodology to all password lengths, data fusion techniques are employed to standardize the input data from different datasets with different password lengths. Experimental evaluation has shown that the proposed GAFMAT method achieved an equal error rate of 0.04545 in the CMU dataset, indicating that it is considerably outperforming other non-image to image transformation methods. In addition, advanced multidimensional visualization techniques provide support for cybersecurity decision making. The results underscore the effectiveness and practical applicability of the presented approach in enhancing cybersecurity for critical infrastructure.

Keystroke dynamics	Distinctive typing patterns exhibited by individuals during password entry
Keystroke behavior	Specifically related to the way users interact with the keyboard, characterized by timing and rhythm
Typing pattern	Refers to the distinctive behavioral characteristics exhibited by an individual during typing, including factors such as keystroke timing, key hold durations, and inter-key intervals, forming a unique biometric signature
Anomaly detection	Methods used to detect deviations from established typing patterns, indicating possible unauthorized access
Insider threat	The potential for an insider to use their authorized access or knowledge of an organization to cause harm
Siamese Neural Network (SNN)	A neural network architecture consisting of two or more identical subnetworks sharing parameters and weights, designed to compare input pairs and measure similarity or difference
Equal Error Rate (EER)	A performance metric in biometric and authentication systems, representing the point where false acceptance and false rejection rates are equal
Convolutional Neural Network (CNN)	A class of deep learning models designed to process data such as images by applying convolutional operations to extract hierarchical features for tasks like classification, detection, and segmentation

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Today's cyber environment provides cybercriminals and intruders with many opportunities to attack national networks and critical infrastructure, demand ransom for data, engage in large-scale fraud schemes, and threaten national security. The consequences of these threats can be severe and result in significant financial loss, reputational damage, and loss of customer trust. Cybersecurity threats are evolving at such a pace that traditional password-based methods are not keeping up with the competition. Although passwords remain the most common form of authentication, they are often subject to phishing, brute force, social engineering, or insider misuse attacks, resulting in massive data breaches and financial losses. These problems are particularly relevant to critical infrastructure systems, which include industries such as power grids, transportation, healthcare, finance, and defense. When insiders gain unauthorized access to critical facilities, the consequences go far beyond financial loss; they can disrupt essential services and pose serious national security risks [36, 84].

Stolen credentials account for 80% of the financial losses attributed to cybercrime [105]. Phishing is a form of cyberattack that uses fraudulent emails, text messages, and phone calls, masquerading as messages from a trusted institution, to steal personal, financial, or credential information from an unwary recipient [12, 51]. Multi-factor authentication has become a recommended cybersecurity practice to combat these threats. However, even multi-factor authentication can be undermined if passwords are weak, reused, or stolen. Recent research shows that weak or compromised passwords account for a significant percentage of leaks, reinforcing the need for additional layers of protection [37, 105]. Behavioral biometrics offers a powerful second line of defense. In particular, keystroke dynamics allow users to be authenticated by analyzing subtle aspects of their input, such as rhythm, timing, and pressure, without the need for specialized hardware. The keystroke dynamics approach captures various aspects of typing behavior, including the timing of key presses and releases, the typing speed and rhythm. These are then analyzed to create a unique biometric profile for each user. This profile can be employed to continuously monitor and verify user identity, thereby providing an effective means to detect and prevent unauthorized access to critical systems and data. Despite these advantages, keystroke

authentication faces serious problems. High variability as a result of fluctuating typing behavior due to factors such as stress, user posture, or environmental conditions. Methods must consider different passwords, user populations, and real-time conditions without excessive false positives or false negatives. Recent advances in deep learning have greatly improved the ability to learn complex user characteristics from keystroke data. Unlike traditional machine learning methods, which often rely on manually created features or may have difficulty detecting complex patterns, deep learning architectures can automatically extract subtle temporal and spatial features.

This thesis focuses on static authentication, which requires users to enter passwords in a characteristic manner, rather than continuous authentication. While continuous methods have their merits, static approaches remain the baseline for many systems in critical infrastructure, facilitating direct comparison with previous literature using certain quality assessment metrics such as equal error rate [56]. By combining advanced deep learning models with image-based data transformation and robust data fusion, this thesis aims to demonstrate how an authentication system can accommodate different passwords and users, thereby strengthening the security of critical infrastructure.

Research Problem

Protecting critical infrastructure systems such as power grids, transportation networks, and communications services is critical to public safety, economic stability, and national security. These systems increasingly face cyberattacks that exploit weaknesses in authentication mechanisms [36]. While passwords are common access control methods, they are inadequate against advanced threats like credential theft. Insider attacks pose significant dangers, as insiders with legitimate access can abuse their privileges. Current password-based systems depend on static information, which attackers can often obtain, necessitating dynamic behavior-based authentication.

The primary research problem in this dissertation is the limitations of traditional authentication methods. For instance, passwords can be easily stolen, captured by keyloggers, or compromised through social engineering attacks, making them very vulnerable. These methods fail to effectively prevent unauthorized access and insider threats in

high-security environments.

Keystroke dynamics is a form of behavioral biometrics, offers a promising alternative by analyzing unique typing patterns for continuous identity verification. However, several challenges prevent its direct application in critical infrastructure. First, natural typing behavior depends on physical, environmental, and situational factors, making it difficult to develop accurate models. Second, insider threats, where legitimate users intentionally abuse their privileges, are particularly difficult to detect when relying only on static credentials or traditional security measures. Finally, critical infrastructure systems often have multiple password lengths, making it difficult to train and deploy models. Models must adapt to different users, password complexity, and real-time operation without affecting accuracy.

This thesis addresses these challenges by investigating how deep learning, in particular Siamese Neural Networks (SNNs) combined with Convolutional Neural Networks (CNNs), can transform numerical keystroke patterns into image formats, thereby reducing the equal error rate and enhancing authentication. The system must remain robust to different users, password lengths, and operating conditions, ensuring practical use in high-security environments. By addressing these challenges, we aim to develop a secure keystroke-based authentication system that protects against external cyberattacks and internal threats in critical infrastructure environments.

Actuality

National and international cybersecurity efforts are increasingly focused on protecting critical infrastructure, such as energy, transportation, and communications systems, from insider threats and cyber attacks [22]. In the Baltic states, exercises such as Locked Shields, organized by NATO's Cooperative Cyber Defence Center of Excellence, underscore the importance of being prepared to confront sophisticated adversaries. Similarly, Lithuanian cybersecurity institutions, including the National Cyber Security Center (NCSC) under the Ministry of National Defense, emphasize that the resilience of critical infrastructure is important not only for national security, but also for sustainable development and public welfare [19]. In this context, keystroke dynamics has become a particularly relevant form of behavioral biometrics to protect high-

value systems. By analyzing individual typing patterns such as timing, speed, and rhythm, methods based on keystroke dynamics allow for continuous verification of a user's identity without requiring specialized hardware. This approach is cost-effective and affordable, enabling real-time detection of unauthorized access. Moreover, machine learning, especially deep learning, has significantly improved keystroke analytics using SNN with CNNs branches are excellent at detecting nuances in large keystroke datasets [29, 52, 117]. Branches are identical convolutional neural network nodes in the Siamese neural network architecture, used to simultaneously process and extract meaningful features from the input data for efficient comparison of similarities. Thus, these models can improve both the authentication accuracy and the insider threat detection performance.

Research Object

The research object of the study is as follows:

- User-generated keystroke biometric data, methods for identifying insider threats and preventing unauthorized activities to improve end-to-end cybersecurity.
- A deep learning-based user authentication system for critical infrastructure, utilizing keystroke dynamics and Siamese neural networks with a triplet loss function.
- Methods for transforming keystroke data into visual representations.

Research Aim and Objectives

The aim of this thesis is to develop and evaluate an advanced deep learning-based methodology to detect insider threats within critical infrastructure systems based on keystroke dynamics. This methodology aims to improve the detection of insider threats and unauthorized access by transforming non-image or tabular keystroke data into image representations and standardizing multiple passwords of different lengths by interpolation-based data fusion. It also presents a novel approach to user authentication based on keystroke dynamics, leveraging an SNN architecture with CNNs branches.

In order to achieve the aim of this thesis, the following **objectives** must be accomplished:

1. Conduct a comprehensive analytical review of user authentication methods used in critical infrastructures, with a particular focus on behavioral biometrics, especially keystroke dynamics.

2. To evaluate deep learning techniques and performance metrics for insider threat detection by analyzing users' keystroke typing behavior when entering passwords, and to assess their impact on improving user authentication accuracy.

3. To propose a novel user authentication methodology based on keystroke dynamics, utilizing insights from behavioral biometrics and deep learning techniques, and fusing multiple passwords of different lengths to enhance threat detection in critical infrastructure systems.

4. To evaluate the effectiveness of the proposed methodology using publicly available keystroke dynamics datasets.

Research Methods

This thesis employs literature review, data transformation techniques, and advanced machine learning models, with a particular focus on keystroke dynamics authentication for enhancing cybersecurity in critical infrastructure systems. The research methods adopted in this thesis are outlined below:

1. Literature review. A comprehensive literature review was conducted to identify existing methods for anomaly detection and insider threat prevention in critical infrastructure, specifically in user authentication through behavioral biometrics. The review focused on deep-learning based techniques, keystroke dynamics, and the challenges of applying these methods in high-security environments.

2. Development non-image to image methods. To ensure consistency in model training and enhance data compatibility with deep-learning based methods, keystroke data were transformed

from non-image/tabular formats into image representations using methods such as Gramian Angular Summation Field (GASF), the Gramian Angular Difference Field (GADF), the Markov Transition Field (MTF), and the Recurrence Plot (RP) methods, GAbor Filter MAtrix Transformation (GAFMAT).

3. Deep-learning based model development. The core of this research involves the development of a deep learning-based model for user authentication. An SNN architecture, consisting of two or more identical sub-networks, was chosen for its ability to compare two inputs and learn to distinguish legitimate users from potential intruders based on their typing patterns.

4. Applications of dimensionality reduction methods. Principal Component Analysis (PCA), t-distributed Stochastic Neighbor Embedding (t-SNE), and Uniform Manifold Approximation and Projection (UMAP).

5. Data standardization. To accommodate the varying lengths of passwords and their corresponding keystroke dynamics data, the GAFMAT method was applied to standardize the data. This transformation not only transforms the keystroke time series into images but also ensures consistency across datasets of varying dimensions. Linear interpolation was used to resize and normalize images, which facilitated the training of SNNs with CNNs branches by providing uniform input dimensions.

6. Experimental design and evaluation. The developed methodology was evaluated through a series of experimental studies on publicly available datasets. The model's performance was measured using key performance indicators such as Equal Error Rate (EER), accuracy, and Area Under the Curve (AUC) to assess the effectiveness of the authentication system.

7. Comparative analysis. A comparative analysis was conducted to benchmark the performance of the proposed system against other state-of-the-art methodologies. This analysis focused on evaluating the system's adaptability to varying password lengths, real-time detection of anomalies, and its ability to differentiate between legitimate users and potential attackers. The findings of

these experiments were used to fine-tune the system and improve its generalizability across different security contexts.

Scientific Novelty

This thesis presents several novel contributions to the field of user authentication and cybersecurity, with a specific focus on detecting insider threats in critical infrastructure systems using keystroke dynamics and advanced deep learning techniques. The main contribution of this thesis is the development and evaluation of a deep learning methodology for detecting insider threats in critical infrastructure systems. This methodology is based on transforming non-image keystroke dynamics data into image representations using the novel GAFMAT. This transformation allows the application of CNN in an SNN architecture. As well, the methodology integrates a solution to standardize keystroke dynamics data for different password lengths and datasets using interpolation and image resizing techniques. Using data fusion techniques to standardize keystroke data across different password lengths and datasets improves the model's ability to generalize across different inputs. Thus, the methodology introduces an image-based approach to user authentication using behavioral biometrics to better detect insider threats and unauthorized access.

The key novelties of this research are as follows:

1. A novel non-image to image data transformation method, GAFMAT, is introduced to enhance feature extraction of keystroke dynamics and improve the performance of user authentication using SNN with CNNs branches.

2. A solution for standardizing keystroke dynamics is developed, addressing variability in datasets by using data fusion, interpolation and image resizing techniques.

3. A comprehensive methodology integrating GAFMAT with deep learning methods is proposed, aimed at insider threat detection within critical infrastructure using fused behavioral biometric data analysis.

Practical Value of the Research

The thesis proposes an enhancement to critical infrastructure security by introducing a more reliable user authentication method based on keystroke dynamics. In contrast to conventional password-based systems, which are susceptible to security breaches, this methodology employs deep learning to analyze distinctive typing patterns, thereby enhancing accuracy and resilience to insider threats. Its practical applicability has been demonstrated through extensive experiments, and the solution can be adapted to real-world scenarios without significantly affecting user experience or system resources.

Utilizing sophisticated models, such as SNN with CNNs branches, the system adeptly differentiates between legitimate users and attackers, while exhibiting adaptability to diverse user behaviors and password lengths. The system's scalability ensures its applicability across a wide range of sectors, including government, military, healthcare, and energy.

The proposed data fusion strategies based on interpolation methods address some of the shortcomings of commonly used keystroke authentication. The proposed methodology does not require specialized sensors or hardware, handles variable password lengths accurately, and adapts to insider threats more effectively than approaches with a fixed length of one particular password. Experimental validation on public datasets confirms the practical effectiveness of the approach, achieving minimal error rates while maintaining usability. This research provides valuable insights for organizations seeking adaptive biometric authentication to strengthen their cybersecurity resilience.

Statements to be Defended

The thesis defends the following statements:

1. Transformation of keystroke dynamics data into image representations, utilizing the new method GAFMAT, enhances the efficacy of the deep learning model in user authentication. By standardizing keystroke data and applying advanced transformation technique, the system is better able to distinguish legitimate users from imposters.

2. The research, which utilized two types of data fusion strategies, time series interpolation and image post-resizing with interpolation, reveals that linear interpolation offers a balanced approach, providing the lowest average equal error rate and demonstrating stable performance across different datasets.

3. The proposed user authentication methodology is intended to be practically applicable in a real critical infrastructure environment. It has been evaluated through experimental studies using publicly available datasets, which demonstrate applicability, versatility, and enhanced security in user authentication in various scenarios.

Approbation of the Research Results

The results obtained in this thesis were disseminated through publications and conference presentations. The research findings have been published in 5 research papers: 3 papers in periodic scientific journals indexed by Clarivate Web of Science (WoS); 2 papers in peer-reviewed scientific conference proceedings. The results were presented at 2 international and 4 national scientific conferences.

Articles published in international research journals with a citation index in the Clarivate WoS database:

1. Budžys, Arnoldas; Kurasova, Olga; Medvedev, Viktor. Deep Learning-Based Authentication for Insider Threat Detection in Critical Infrastructure // *Artificial Intelligence Review*. Dordrecht : Springer Nature B.V. ISSN 0269-2821. eISSN 1573-7462. 2024, vol. 57, iss. 10, art. no. 272, p. 1–35. DOI: 10.1007/s10462-024-10893-1.

2. Budžys, Arnoldas; Medvedev, Viktor; Kurasova, Olga. Integrating Deep Learning and Data Fusion for Advanced Keystroke Dynamics Authentication // *Computer Standards & Interfaces*. Amsterdam : Elsevier B.V. ISSN 0920-5489. 2025, vol. 92, art. no. 103931, p. 1–14. DOI: 10.1016/j.csi.2024.103931.

3. Kurasova, Olga; Budžys, Arnoldas; Medvedev, Viktor. Exploring Multidimensional Embeddings for Decision Support Using Advanced Visualization Techniques // *Informatics*. Basel : MDPI.

eISSN 2227-9709. 2024, vol. 11, iss. 1, art. no. 11, p. 1–17. DOI: 10.3390/informatics11010011.

Papers in peer-reviewed scientific conference proceedings:

1. Medvedev, Viktor; Budžys, Arnoldas; Kurasova, Olga. Enhancing Keystroke Biometric Authentication Using Deep Learning Techniques // *2023 18th Iberian Conference on Information Systems and Technologies (CISTI), 20–23 June, Aveiro, Portugal, 2023* : proceedings. New York : IEEE, 2023. ISBN 9798350305272. eISBN 9789893347928. ISSN 2166-0727. p. 1–6. DOI: 10.23919/CISTI58278.2023.10211344.

2. Budžys, Arnoldas; Kurasova, Olga; Medvedev, Viktor. Behavioral Biometrics Authentication in Critical Infrastructure Using Siamese Neural Networks // *HCI for cybersecurity, privacy and trust: 5th international conference, HCI-CPT 2023, held as part of the 25th HCI international conference, HCII 2023. Copenhagen, Denmark, July 23–28, 2023* : proceedings. Cham : Springer, 2023. ISBN 9783031358210. eISBN 9783031358227. p. 309–322. (Lecture notes in computer science, ISSN 0302-9743, eISSN 1611-3349 ; vol. 14045). DOI: 10.1007/978-3-031-35822-7_21.

Abstracts in conference proceedings:

1. Budžys, Arnoldas; Medvedev, Viktor; Kurasova, Olga. User Behavior Analysis Based on Similarity Measures to Detect Anomalies // *DAMSS: 12th conference on data analysis methods for software systems, Druskininkai, Lithuania, December 2–4, 2021*. Vilnius : Vilnius University Press, 2021. ISBN 9786090706732. eISBN 9786090706749. p. 8. DOI: 10.15388/DAMSS.12.2021.

2. Budžys, Arnoldas; Kurasova, Olga; Medvedev, Viktor. Deep Learning-Based Prevention of Insider Threats Using User Behavioral Keystroke Biometrics // *EURO 2022: [32nd European Conference on Operational Research (EURO XXXII)], Espoo, Finland, July 3–6, 2022* : abstract book. Espoo : Aalto university, 2022. ISBN 9789519525419. p. 144. Prieiga per internetą: <https://www.euro-online.org/conf/admin/tmp/program-euro32.pdf>.

3. Budžys, Arnoldas; Kurasova, Olga; Medvedev, Viktor. Intrusion Detection Based on Keystroke Biometrics and Siamese Neural Networks // *DAMSS: 13th conference on data analysis methods for software systems, Druskininkai, Lithuania, December 1–3, 2022*. Vilnius : Vilnius University Press, 2022. ISBN 9786090707944. eISBN 9786090707951. p. 13. (Vilnius University Proceedings, eISSN 2669-0233 ; vol. 31). DOI: 10.15388/DAMSS.13.2022.

4. Budžys, Arnoldas; Kurasova, Olga; Medvedev, Viktor. Insider Threat Detection: A New Keystroke Dynamics-Based Approach to User Authentication in Critical Infrastructure // *DAMSS: 14th conference on data analysis methods for software systems, Druskininkai, Lithuania, November 30–December 2, 2023*. Vilnius. Vilnius : Vilniaus universiteto leidykla, 2023. eISBN 9786090709856. p. 16. (Vilnius University Proceedings, eISSN 2669-0233 ; vol. 39). DOI: 10.15388/DAMSS.14.2023.

5. Budžys, Arnoldas; Medvedev, Viktor; Kurasova, Olga. Enhancing Cybersecurity Using Keystroke Dynamics and Data Fusion Techniques // *DAMSS: 15th conference on data analysis methods for software systems, Druskininkai, Lithuania, November 28–30, 2024*. Vilnius : Vilniaus universiteto leidykla, 2024. eISBN 9786090711125. p. 14. (Vilnius University Proceedings, eISSN 2669-0233 ; vol. 52). DOI: 10.15388/DAMSS.15.2024.

Presentations in international scientific conferences:

1. Budžys, Arnoldas. Deep Learning-Based Prevention of Insider Threats Using User Behavioral Keystroke Biometrics. EURO 2022: 32nd European Conference on Operational Research (EURO XXXII), Espoo, Finland, July 3–6, 2022.

2. Budžys, Arnoldas. Behavioral Biometrics Authentication in Critical Infrastructure Using Siamese Neural Networks. HCI for Cybersecurity, Privacy and Trust: 5th international conference, HCI-CPT 2023, held as part of the 25th HCI international conference, HCII 2023. Copenhagen, Denmark, July 23–28, 2023.

Presentations in national scientific conferences:

1. Budžys, Arnoldas. User Behavior Analysis Based on Similarity Measures to Detect Anomalies. DAMSS: 12th conference on data analysis methods for software systems, Druskininkai, Lithuania, December 2–4, 2021.

2. Budžys, Arnoldas. Intrusion Detection Based on Keystroke Biometrics and Siamese Neural Networks. DAMSS: 13th conference on data analysis methods for software systems, Druskininkai, Lithuania, December 1–3, 2022.

3. Budžys, Arnoldas. Insider Threat Detection: A New Keystroke Dynamics-Based Approach to User Authentication in Critical Infrastructure. DAMSS: 14th conference on data analysis methods for software systems, Druskininkai, Lithuania, November 30–December 2, 2023.

4. Budžys, Arnoldas. Enhancing Cybersecurity Using Keystroke Dynamics and Data Fusion Techniques. DAMSS: 15th conference on data analysis methods for software systems, Druskininkai, Lithuania, November 28–30, 2024.

Outline of the Thesis

This dissertation is organized into three main chapters, followed by general conclusions and a bibliography.

- Chapter 1 provides a detailed literature review, focusing on machine learning techniques in keystroke dynamics, including SNNs, data standardization, and visualization methods. This chapter sets the foundation for the research and explores the state-of-the-art methods relevant to user authentication using keystroke dynamics.

- Chapter 2 introduces the proposed methodology for user authentication, with an emphasis on the architecture of SNNs, the transformation of tabular keystroke data to image-based time series, and the application of GAFMAT. This chapter also covers the proposed data visualization and data fusion techniques used for decision support in user authentication.

- Chapter 3 presents the experiments and results obtained from the application of the proposed methodology. This includes the evaluation of keystroke dynamics using performance metrics and the experiments conducted on different datasets (CMU, GREYC-NISLAB, KeyRecs), along with data visualization and data fusion experiments for user authentication. A detailed discussion of the findings and validation of the data fusion results is also provided.
- Finally, the key findings of the research are summarized in the general conclusions section, followed by a comprehensive bibliography.

The thesis consists of 165 pages, with the summary in Lithuanian starting from page 140. It includes 24 figures, 15 tables, and 2 algorithms.

Ensuring the security of critical infrastructure systems, including power grids, transport networks, and communications systems, is essential to maintain stability and continuity of society. There is publicly available historical evidence that cyberattacks on critical infrastructure can have extremely negative consequences [36]. These systems are increasingly being targeted by cyberthreats that attempt to exploit weaknesses in authentication mechanisms [67]. The safety and availability of these vital services depend on robust security protocols in which authentication plays a critical role in distinguishing legitimate access from unauthorized intrusion. Traditional password-based authentication systems are often vulnerable to various types of attacks, including brute-force attacks, phishing, and credential overloading. Although the complexity and length of the password can improve security, they also pose challenges in terms of user experience and system performance. In addition, the variability in password length and related keystroke dynamics poses additional challenges in training machine learning models, which are effective at identifying nuances in data for authentication purposes. Keystroke Dynamics analyses individual typing behavior, such as speed, rhythm, and keystroke intervals, to authenticate users. This method captures subtle differences in typing behavior and allows user identity verification without the need for special equipment. Credential dumping [78] is a cyberattack in which fraudsters steal or otherwise obtain account credentials to gain access to user accounts in various applications.

Insiders are adversaries, individuals, groups, or organizations that attempt to compromise the security of critical infrastructures and possibly disrupt their operations. Insiders can cause damage to systems by exploiting their access. They are often disgruntled employees who have access to both the facility and the network. They basically use their knowledge and access level as a tool to perform their actions. Detecting insiders is challenging because attackers have specific knowledge, capabilities, and authorized access to systems. The insider threat is considered one of the biggest threats to information security, but is often overlooked [108].

Recent research highlights keystroke dynamics as a promising method of enhancing authentication, since attackers cannot easily repli-

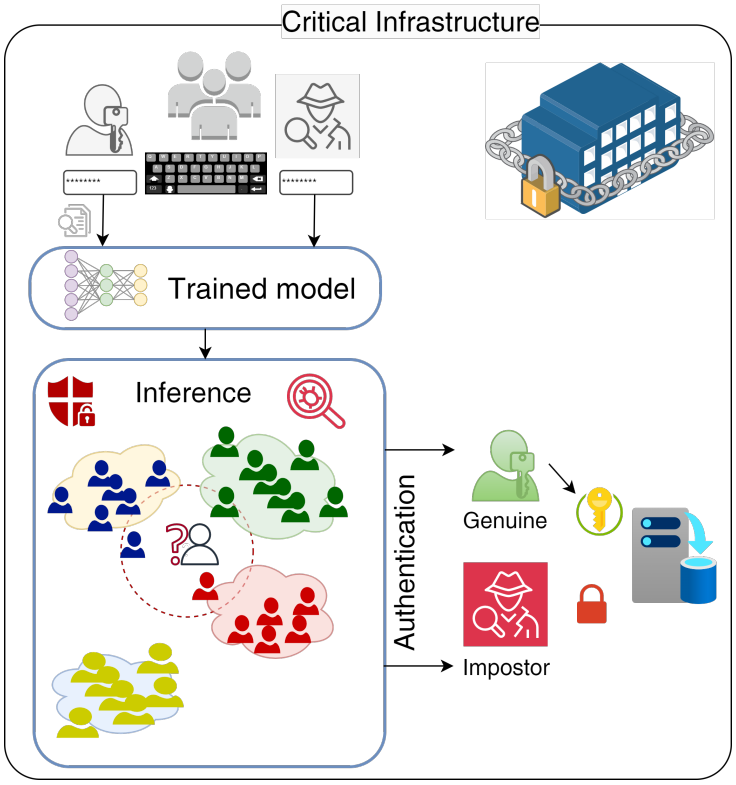


Figure 1.1: Illustrative example of a user authentication scenario in a critical infrastructure environment using keystroke dynamics

cate an individual's typing behavior, even if they have obtained the password. The authentication process, as illustrated in Figure 1.1, starts with the user entering a password, which the system transmits to a trained deep learning model for inference. The trained model, based on keystroke data, classifies users according to their keystroke typing characteristics and outputs an embedding that can be compared against reference embeddings of known authorized users. When the input aligns with the behavior of a legitimate user, the system grants access to critical infrastructure; otherwise, it detects the attempt as a spoof and denies entry, thus safeguarding these systems against unauthorized intrusion.

1.1. Insights Into Cybersecurity and Keystroke Dynamics Research in Lithuania

Cybersecurity research in Lithuania has gained particular interest in recent years, with a focus on behavioral biometrics and critical infrastructure protection. Keystroke dynamics, as a form of behavioral biometrics, offers a promising approach to improving the cybersecurity of critical systems by identifying users by their unique typing. However, recent research shows that even advanced biometric authentication methods face growing challenges from sophisticated attacks such as keystroke injection payloads [45], which use deep learning models to replicate legitimate user behavior and bypass security systems. The research carried out by Augutis et al. [9] focused on assessing the criticality of the energy infrastructure, especially in the heat and electricity sectors. These researchers emphasized the importance of assessing the "interdependencies" between infrastructure sectors to determine their vulnerability. This helps to understand how breaches in one sector can lead to broader problems, which emphasizes the importance of developing robust cybersecurity solutions for critical systems [81].

Various exercises are conducted to test the protection of critical infrastructure in the Baltic States, the best known of which is the Locked Shields cyber defense exercise organized by the NATO Cooperative Cyber Defence Centre of Excellence every year since 2010 [22]. Amber Mist is an international cyber defense exercise organized annually by the Lithuanian Armed Forces since 2013. The exercise plays an important role in strengthening Lithuania's cybersecurity capabilities and promoting international cooperation in this area. The Amber Mist exercise uses a complex structure that simulates real-life cyberthreats, including at critical infrastructure targets. The red team acts as the "bad guys", developing and executing cyberattack scenarios. The blue team represents the defenders, tasked with identifying, analyzing and preventing cyber incidents. The exercise tests a variety of scenarios, including disrupting communications, insider attacks, installing malicious code, and hacking into a physical network. These scenarios are designed to assess the ability of the military, government agencies, and private companies to effectively respond to cyberthreats. The research by Bukauskas et al. [16] focused on remapping cybersecurity competences in Lithuania. They

examined the evolving needs of the cybersecurity workforce and proposed updates to educational programs and professional development frameworks.

The growing cyber threats in the Baltic Sea region pose a significant risk to critical infrastructure, potentially disrupting essential services and economic activity. The State Security Department of the Republic of Lithuania and the Second Investigation Department under the Ministry of National Defence of the Republic of Lithuania in the annual Threats to National Security Report state that Lithuania constantly faces various types of cyber incidents aimed at compromising the country's information resources, critical infrastructure of national security significance [54]. As the National Cyber Security Center (NCSC) under the Ministry of National Defense, the main Lithuanian cybersecurity institution responsible for unified management of cyber incidents, notes [19], the resilience of critical infrastructure is not only a matter of national security, but also a foundation for sustainable development and public welfare. The NCSC Regional Cyber Defense Center's 2024 report also points out that behavioral analytics, machine learning and artificial intelligence can help identify anomalies and suspicious activity indicative of zero-day exploits. For example, analyzing network traffic can identify unusual patterns that may indicate an ongoing zero-day attack, enabling rapid response and remedial action.

1.2. Enhancing User Authentication with Keystroke Biometrics

The origins of keystroke biometrics can be traced back to telegraph operators in the 1880s, who were able to recognize each other based on their unique tapping patterns [59]. Traditional authentication systems rely on the use of a password or PIN, known only to the user. The system does not store the password itself, but only the cryptographic hash of the password, and verifies the user's identity by comparing the hash of the entered password with the stored hash. In such systems, security depends on the shared secret remaining confidential; however, if the password is leaked, it becomes relatively easy for an attacker to impersonate the legitimate user.

Passwords are something you "know" making them easy to remember but difficult for insiders to guess. However, in practice, users often share passwords, reuse them on multiple platforms, or choose weak

credentials that are easily guessed or extracted. Exploiting these vulnerabilities, threat vectors such as masquerading and identity theft attacks have become widespread. As cyberattacks and cyberfraud continue to impact our daily lives, the FBI's Internet Crime Complaint Center (IC3) plays an essential role in dealing with cyberthreats. IC3 serves as a public resource for reporting cyberattacks and incidents, allowing them to collect data, identify trends, and address threats at hand. In 2022, IC3 received 800,944 complaints, a 5% decrease from 2021. However, the potential total loss increased from $6.9 billion in 2021 to more than $10.2 billion in 2022 [37]. The latest data from cybersecurity Ventures indicates that cybercrime is expected to cost the global economy around $8 trillion in 2023. This represents a significant increase in global cybercrime costs, which have been growing annually at around 15%. The growing cyberthreats impact various sectors, from small businesses to critical infrastructure like utilities and hospitals [104]. The Verizon 2023 Data Breach Investigations Report [105] emphasizes that stolen credentials remain one of the top attack vectors for gaining unauthorized access to systems. According to the report, 44.7% of attackers use stolen credentials, marking a slight increase from previous years. These credentials are often exploited in combination with other methods, such as ransomware and social engineering, to breach systems. In the last two years, such attacks have tripled. These facts show that the traditional password-based authentication scheme is insecure, expensive, and inconvenient.

In the field of cybersecurity, the deployment of security information and event management systems is essential for organizations to proactively detect and address security threats to protect their business operations. Network-based Intrusion Detection Systems (NIDS) and host-based Intrusion Detection Systems (HIDS) play key roles in ensuring robust cybersecurity. NIDS monitors network traffic for anomalies, while HIDS focuses on individual systems, detecting unusual activity or policy violations, including insider threats. A major problem for IDS is data imbalance, especially when detecting rare attacks such as zero-day attacks. The paper [7] introduced a new process to refine density-based spatial clustering of applications with noise by incorporating novel cluster distance measurements. In addition, [11] explored the use of machine learning techniques to improve the performance of NIDS in detecting

anomalous network flows. By carefully analyzing system activity and user behavior, HIDS can identify potential security breaches within an organization, including those committed by insiders [6].

To fight back with these attacks additional layer of security controls must be developed to distinguish between a legitimate user and an imposter without negatively impacting the user's experience. This approach aims to increase security by integrating multi-factor authentication based on physiological or behavioral biometrics, such as fingerprint scanners, voice authentication, iris recognition or keystroke dynamics, mouse movement dynamics, voice recognition, signature analysis. These solutions provide a high level of security. However, deploying physiological biometrics authentication solutions often requires the purchase and installation of new, potentially costly hardware and has several disadvantages. Facial recognition can be affected by hats, glasses, and changes in hairstyle. Iris recognition can be deceived by photographs. Furthermore, fingerprints can be replicated to impersonate another person [2]. In today's wars, phones are accessed using the physiological biometric data of the deceased person to take their money or cause damage to their social networks [43, 101].

Conversely, behavioral biometrics offers a pragmatic solution by monitoring the distinctive manner in which users interact with the keyboard, providing a seamless and continuous layer of authentication. Additionally, user identification methods such as keystroke dynamics, mouse movement dynamics, voice recognition are becoming increasingly accurate over time in identifying the actual user and do not require additional hardware to implement such authentication methods. These advancements in behavioral biometrics contribute to more precise and reliable authentication, enhancing overall security without compromising the user experience [47, 61].

Keystroke dynamics is a form of behavioral biometrics that analyses the way users interact with the keyboard [66]. This analysis focuses on a number of variables, including typing speed, key hold duration, and keystroke intervals. This method represents a distinctive approach to user authentication, based on the analysis of their typical typing patterns. Keystroke dynamics can be classified into two categories: static authentication keystroke dynamics, where typing patterns are analyzed at the time of logging in by entering a password, and continuous authen-

tication keystroke dynamics, where typing patterns are continuously analyzed throughout the session after logging in [23]. The relative merits and drawbacks of each method vary depending on the specific context and the desired level of security. Static authentication is typically employed during the initial login phase, where the user is prompted to enter a known password or phrase. The system compares the user's typing behavior to previously recorded patterns, making this method straightforward and computationally efficient. The principal advantage of this method is its simplicity, in that the system is only required to verify the user during the login process. However, a significant limitation of this approach is that it does not provide continuous security, making the system susceptible to attack after initial authentication. An adversary who gains access after authentication may remain undetected, as no further monitoring of the user's behavior occurs throughout the session.

In contrast, dynamic authentication provides an additional layer of security by continuously monitoring user's typing patterns throughout the session. This method holds significant value in high-security environments, where the threat of account breaches remains a critical concern even after initial authentication. Continuous authentication systems are capable of detecting anomalous behavior that may indicate the presence of an unauthorized user, thereby providing real-time responses to potential threats. However, the implementation of dynamic systems is more complex and resource-intensive. Such systems require continuous aggregation and real-time examination of data, which can result in performance bottlenecks and difficulties in maintaining a lower Equal Error Rate (EER) [23]. EER is a performance metric in biometric authentication systems that represents the point where the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) are equal. A lower EER indicates a better balance between security and usability, making it a critical measure for evaluating the effectiveness of authentication methods.

In assessing the efficacy of these methodologies, the precision of static authentication is of paramount importance. In the event that static authentication does not produce a high level of accuracy or a low EER [40, 41, 56, 93, 98, 113], there is minimal value in pursuing more complex continuous authentication, as the foundation for distinguishing

legitimate users from imposters is already flawed.

The efficacy of continuous authentication depends on the reliability of the initial static authentication. It is therefore imperative to achieve optimal accuracy in static authentication before implementing more advanced continuous systems. In the absence of this, the additional complexity of continuous authentication may not yield meaningful security benefits, as any gaps in the initial verification process would compromise the overall system. Therefore, it is imperative that research efforts prioritize the refinement of static authentication methods before progressing to more sophisticated dynamic approaches. Table 1.1 offers a comprehensive comparison of keystroke dynamics approaches and authentication technologies in cybersecurity.

Despite the ubiquity of password-based authentication, the efficacy of this method is undermined by the prevalence of weak or frequently reused credentials. This assertion is substantiated by the escalating reports of stolen credentials in cyberattacks. In response, organizations have been working to strengthen security by deploying additional protection mechanisms such as intrusion detection systems and multifactor authentication. However, these systems face their own operational challenges, including complexity, resource intensity, and occasional false alarms. A promising alternative that does not require additional hardware is keystroke biometrics, a behavioral approach analyzing typing speed and rhythm [99]. When used in the login stage, keystroke-based static authentication must achieve a low EER to ensure an effective balance between security and user convenience. This emphasizes the importance of refining these foundational methods before implementing more advanced authentication strategies.

1.3. Machine Learning in Keystroke Dynamics

In static authentication keystroke dynamics, an individual's identity is authenticated through the examination of their typing patterns when entering a predefined password or passphrase. Several publicly available datasets have been extensively used for the development and evaluation of keystroke dynamics-based authentication systems, including the CMU dataset [56], GREYC-NISLAB [41], and KeyRecs [26] (Subsection 2.2.1). The CMU dataset has become a foundational resource in this research area due to its comprehensive collection of samples per

Table 1.1: A comparative analysis of keystroke dynamics and authentication technologies in cybersecurity in related works

Reference	Methodology Used	Dataset	Security Field	Auth. Mode	Accuracy Metric
[56]	anomaly-detection algorithms, distance functions	CMU	Keystroke Dynamics Authentication (KD Auth.)	static	EER, zero-miss rate
[116]	distance functions	CMU	KD Auth.	static	EER
[73]	inductive transfer encoder	CMU	KD Auth.	static	EER
[18]	CNN	CMU, GREYC labs	KD Auth.	static	EER
[49]	k-NN-based	CMU	KD Auth.	static	EER
[76]	machine learning, deep learning	CMU	KD Auth.	static	Accuracy
[57]	XGBoost	CMU	KD Auth.	static	Accuracy
[62]	CNN	CMU	KD Auth.	static	FAR, Accuracy
[10]	instance-based algorithms, distance functions	Clarkson II, Buffalo	KD Auth., intrusion detection	dynamic	EER
[3]	behavioral biometrics	various behavioral datasets	behavioral biometrics	dynamic	EER, FAR, FRR
[65]	CNN, RNN	Clarkson II, Buffalo	KD Auth.	dynamic	EER
[98]	XGBoost	CMU	KD Auth.	static	Accuracy
[4]	Siamese RNN	Aalto keystroke data	KD Auth.	dynamic	EER
[11]	machine learning, classification algorithms	network intrusion detection data	network security	dynamic	Recall
[95]	CNN	Real-World PPG datasets	biometric identification	static	Accuracy
[69]	statistical techniques, machine learning	UEBA dataset	behavior analytics	static	EER
[6]	machine learning	synthetic datasets, CERT dataset	insider threat detection	N/A	F-score, TNR, FPR, AUC
[87]	machine learning, distance functions	CMU	KD Auth.	static	FAR, FPR, EER
[82]	deep learning	GREYC-NISLAB	KD Auth.	static	EER
[A.2]	GAFMAT and SNN	CMU, GREYC-NISLAB	KD Auth.	static	EER, Accuracy

individual.

Different machine learning methods with different approaches and their respective performance in the CMU dataset are summarized in Table 1.2. These results demonstrate how the choice of algorithm and different network training strategies significantly affect authentication accuracy [C.1]. Notably, the CMU dataset's baseline evaluation reported an EER of 9.6% [56].

Table 1.2: Average EER of different approaches for different machine learning methods.

Methods	**Average EER**		
	Strategie 1	Strategie 2	Strategie 3
Nearest Neighbour	0.3795	0.4548	0.5013
Euclidean	0.1693	0.1863	0.2346
Manhattan	0.1503	0.1622	0.2032
Manhattan (Scaled)	0.0945	0.0986	0.1291
Manhattan (Filtered)	0.1253	0.1399	0.1886
Mahalanobis	0.1596	0.1987	0.2338
Euclidean (Normed)	0.2107	0.2308	0.2483
Mahalanobis (Normed)	0.1996	0.2686	0.3083
Outlier (Counting)	0.1031	0.1060	0.1687
k Means	0.1533	0.1721	0.2238
SVM	0.1205	0.1077	0.1478
Original paper [56]	0.0960		

In the DeepSecure study [66], researchers achieved an EER of 3% using a 4-layer Multi-Layer Perceptron (MLP) that was trained separately for each user. The model was trained using 200 legitimate samples and five imposter samples per user. For instance Çeker and Upadhyaya [18] utilized a convolutional neural network model, achieving a markedly lower EER of 2.3% by augmenting the dataset with synthetic samples. Without augmentation, the EER was 6.5%, highlighting the importance of data processing techniques in improving model performance. Other researchers have used accuracy rates instead of EERs when evaluating user classification models based on keystroke dynamics. For example, XGBoost methods have been shown to achieve user authentication accuracies in excess of 93% [98]. Another noteworthy approach involved using a feed-forward multilayer neural network, employing resilient backpropagation, which resulted in an accuracy of 94.7% [40]. Despite

these advancements, one key limitation of static authentication methods is their susceptibility to cyberattacks, as an attacker could potentially learn the specific typing rhythm associated with a password and exploit this to bypass the system [90, 100]. Zhong et al. [116] also explored static keystroke dynamics authentication and proposed a combination of distance metrics, in particular the Mahalanobis and Manhattan distances, to improve classification accuracy, achieving an EER of 8.4% after removing outliers. Similarly, [73] utilized an inductive transfer encoder approach and achieved an EER of 6.3%, demonstrating the ongoing advancements in mitigating the weaknesses of static methods. Furthermore, methods such as dependency clustering with Manhattan distance [49] and scaled Manhattan distance combined with standard deviation [87] have shown EERs of 7.7% and 9.16%, respectively, indicating that these improvements can bring static authentication closer to the practical deployment level. Nevertheless, the results achieved on the CMU dataset are often based on validation data or rely on the removal of outliers, which may not be representative of real-world usage where user emotions, physical state, and varying environments can significantly affect typing patterns.

Beyond the CMU dataset, other datasets such as GREYC-NISLAB [41] and KeyRecs [26] have also been extensively analyzed. These datasets offer additional resources for researchers aiming to improve the robustness and scalability of static keystroke dynamics systems. For instance, Hazan et al. [47] and Dias et al. [26] evaluated the performance of authentication systems across different behavioral datasets, underscoring the importance of dataset diversity in developing more resilient systems. A detailed comparison of keystroke dynamics methodologies and authentication technologies across various studies, including those focused on different datasets can be found in Table 1.1.

While static keystroke dynamics remains a popular and effective method for user authentication based on behavioral biometrics, it still has its challenges. Machine learning techniques, particularly deep learning models such as CNNs and MLPs, have significantly improved user authentication performance, with EER values dropping to as low as 2.3% for the CMU dataset. However, the potential for cyberattacks and the variability of typing behavior across different sessions remain concerns. Thus, the development of more advanced static models, alongside fur-

ther exploration of continuous authentication methods, will be crucial to enhancing the security and usability of keystroke dynamics-based systems.

1.4. Deep Learning-Based Methods in Keystroke Dynamics

Recently biometric authentication, especially in keystroke dynamics, has been directed towards enhancing the adaptability of deep learning-based models to accommodate the evolving and diverse user interactions with the keyboard. A particularly promising development in this area is the use of SNNs [61, 63, 83]. These networks are specifically designed to measure the similarity between two input samples, making them ideal for tasks such as biometric authentication, where verifying whether two sets of data (e.g., two typing sessions) correspond to the same user is critical. SNNs process inputs through identical sub-networks that share weights and architecture, allowing the model to compare the outputs and assess the similarity between the inputs [80, 117]. This makes SNNs highly effective in recognizing subtle variations in biometric patterns and improving the accuracy of authentication systems based on keystroke dynamics.

Several studies have leveraged SNNs to enhance the performance of keystroke dynamics-based authentication systems. For instance, Hadsell et al. [46] explored the use of contrastive loss functions in SNNs to learn representations that bring similar inputs closer together while pushing dissimilar ones apart. This technique is particularly beneficial for biometric authentication, where a system needs to learn subtle differences between legitimate users and impostors. Furthermore, the introduction of triplet loss functions, as used in models like FaceNet [89], has allowed SNNs to distinguish even finer differences between similar and dissimilar data. The triplet loss function is a metric learning approach used to ensure that embeddings of similar samples are closer together while embeddings of dissimilar samples are farther apart in the feature space.

In keystroke dynamics research, the use of SNNs has gained traction due to their ability to handle imbalanced datasets, a common issue in intrusion detection systems (IDS). SNNs have been successfully applied to this domain to address the class imbalance problem, with promising results in both anomaly detection and multi-class classification tasks [13, 52, 75]. For example, Bedi et al. [13] demonstrated

that SNNs could effectively classify attack types while also identifying normal user behavior in network intrusion scenarios. These studies emphasize the robustness of SNNs in real-time cybersecurity applications, especially in detecting insider threats or unauthorized access using behavioral biometrics like keystroke dynamics. While SNNs are a powerful architecture for comparing two inputs and are particularly well suited for handling imbalanced datasets, they rely on additional neural networks, such as CNNs, to process complex data types effectively. CNNs are particularly effective in the recognition of patterns within images, making them ideal for the extraction of features from visual data. To fully leverage the potential of CNNs in keystroke dynamics research, raw time series data must be transformed into image-like representations. This transformation allows CNNs to extract complex patterns that are often difficult to detect in traditional data formats. This transformation highlights the complementary roles of SNN and CNN and explains the need to convert keystroke data into images.

Keystroke dynamics research involves transforming time series data into image representations, which can be fed into CNN for further processing. Techniques such as the Gramian Angular Summation/Difference Field (GASF/GADF), Markov Transition Field (MTF), and Recurrence Plots (RP) have been employed to convert keystroke data into a visual format, enabling CNNs to extract patterns that are difficult to capture using traditional tabular data formats [24, 35]. This method leverages the strength of CNNs in image classification tasks, allowing for more accurate feature extraction from the transformed keystroke dynamics data.

In the context of cybersecurity, where malicious actors increasingly target user credentials, behavioral biometrics such as keystroke dynamics offer a non-intrusive and effective means of authentication [43]. As traditional password-based systems become vulnerable to phishing and brute-force attacks, integrating keystroke dynamics with deep learning techniques such as SNNs provides an additional layer of security. The ability of SNNs to continuously monitor and adapt to user behavior makes them particularly suitable for IDS, especially in high-risk environments like critical infrastructure protection.

Deep learning-based techniques, and in particular SNNs, have become a powerful tool in biometric authentication, leveraging their ability

to learn and distinguish subtle differences between user actions [61, 117]. These neural networks are particularly good at processing and authenticating based on dynamic features, such as keystroke dynamics, which contain unique temporal patterns for each individual. However, the performance of these networks is significantly dependent on the consistency and quality of the input data. Given the variability in password lengths and keystroke dynamics, it is necessary to standardize input data to optimize the training and performance of SNNs. Various interpolation methods have been proposed to address this challenge [60]. While these methods are mainly used to fill in missing values in the time series, they can also be used to efficiently adapt the length of the time series to a uniform scale [17]. Such standardization involves converting passwords of different lengths into a uniform format, which not only facilitates better training of the model but also improves its generalization ability under different user inputs and scenarios. Importantly, this method plays an important role in detecting insider threats. By standardizing and analyzing keystroke dynamics, SNNs can effectively detect anomalies in user behavior that may indicate malicious activity within an organization. This capability is important for maintaining the security integrity of critical systems where the potential damage from insider threats can be significant.

In summary, the use of deep learning techniques, in particular SNNs, has significantly improved the field of keystroke dynamics authentication. By utilising the ability of SNNs to learn similarity metrics for input samples, researchers have significantly improved the reliability and security of biometric authentication systems. The combination of SNN with CNN and image transformation techniques has opened up new opportunities for improving user authentication in the field of cybersecurity, providing a reliable and scalable solution to protect sensitive information from unauthorized access.

1.5. Methods for Visualization of Keystroke Dynamics Data

To illustrate the challenges and potential solutions for high-dimensional data, consider a dataset characterized by n features. Let's denote the data samples as $X_i = (x_{i1}, \ldots, x_{in})$, $i = 1, \ldots, m$, where each n-dimensional data point $X_i \in \mathbb{R}^n$, $n \geqslant 3$, and m is the number of data samples. The dimensionality reduction aims to find the points $Y_i = (y_{i1}, \ldots, y_{id})$,

$i = 1, \ldots, m$, in a lower-dimensional space ($d < n$), $Y_i \in \mathbb{R}^d$, so that certain properties (such as distances or other proximities between the points) of the dataset are preserved as faithfully as possible. This dimensionality reduction is very important for interpreting data because it transforms the data into a more convenient form. If $d \leqslant 3$ is chosen, the dimensionality reduction allows us to visualize the obtained points in 2D or 3D space. Furthermore, data visualization is crucial for understanding data in decision support systems. By transforming multidimensional data into a more comprehensible and manageable form, dimensionality reduction techniques enable decision-makers to uncover hidden patterns and relationships, leading to more informed decisions. Dimensionality reduction methods can assist in identifying and understanding the unique characteristics of different data clusters, which is crucial for making informed decisions in a decision support system [27, 39].

Visualization is a necessity often not only for analyzing raw data, but also for embeddings generated by deep neural networks such as CNN. Visualization allows researchers and practitioners to gain insight into the learned representations (embeddings), contributing to a deeper understanding of model behavior. This understanding plays a key role in decision making, especially in sensitive applications such as user authentication, medical diagnosis, and autonomous driving, where fast and accurate decisions are of crucial importance. Furthermore, visualization of CNN embeddings helps to identify patterns and anomalies that may not be obvious in high-dimensional space. It allows us to explore the relationships and clusters formed by the embeddings, providing a qualitative assessment of the effectiveness of the model. For example, in user authentication using keystroke dynamics [33], visualization of the embeddings can show how well the model discriminates between different users, which is important for assessing the reliability of an authentication system.

Dimensionality reduction and data visualization techniques are important in machine learning, especially when analyzing complex data [77, 85, 118]. These methods are particularly valuable in exploratory analysis, offering insights into similarity relations in multidimensional data, which is essential for understanding and interpreting neural network embeddings.

Classical methods such as Principal Component Analysis (PCA) [53, 68] and Multidimensional Scaling (MDS) [14, 31, 68] have traditionally been used to reduce dimensionality in data visualization. PCA reduces the dimensionality of the data by identifying orthogonal linear combinations of the original variables (features) that have maximum variance [50]. However, the linear PCA approach may not fully capture the complexity of the nonlinear structures present in the data, which has led to the development of local distance preserving methods such as Local Linear Embedding (LLE) [86] and Isomap [34, 106]. More recent methods such as t-Distributed Stochastic Neighbor Embedding (t-SNE) [103] and Uniform Manifold Approximation and Projection (UMAP) [70] have gained popularity due to their ability to preserve the local structure of high-dimensional data, making them particularly suitable for visualizing embeddings obtained by deep neural networks. These techniques transform multidimensional data into a lower-dimensional space, which not only simplifies data visualization [30, 58, 110], but also improves the computational efficiency of tasks.

As deep learning models, particularly those used in user authentication, generate multidimensional embeddings that are challenging for humans to interpret, the application of dimensionality reduction techniques, such as PCA, t-SNE, and UMAP, becomes crucial. These methods facilitate a more intelligible representation of data, thereby enabling more informed decision-making by preserving salient structures within the dataset while reducing the computational burden. Furthermore, the utilization of visualization techniques serves to enhance the interpretability of deep neural network models, offering insights into the patterns and relationships that exist within the data. The application of these techniques enables researchers to more effectively assess model performance, identify anomalies, and optimize systems in a range of critical applications, including cybersecurity and user authentication.

1.6. Conclusions of the Chapter

The findings from the literature emphasize the urgent need for stronger authentication mechanisms to protect critical infrastructure from sophisticated cyber threats. Traditional password-based authentication is inherently vulnerable, necessitating more advanced solutions. Keystroke dynamics, as a behavioral biometric, offer a viable alternative by leverag-

ing users unique typing patterns without additional hardware requirements.

The integration of deep learning, particularly the combination of SNNs and CNNs, has significantly improved the accuracy and reliability of keystroke-based authentication. These architectures enable effective feature extraction and anomaly detection by transforming keystroke data into more structured representations. However, challenges remain in optimizing these models to minimize false acceptance and rejection rates while ensuring adaptability across diverse real-world conditions.

To fully exploit the potential of keystroke dynamics for cybersecurity in critical infrastructure, future research must address key limitations, including data variability and generalization across different user environments. Furthermore, improving the robustness of the model and validating its performance in large-scale data sets will be essential to establish keystroke-based authentication as a reliable defense against evolving cyber threats. However, keyboard typing patterns can potentially be captured by malicious software, posing significant security risks. To mitigate this threat, specialized informatics engineering approaches should be adopted.

In the emerging field of cybersecurity, especially in times of war [43], there is an increasing demand for advanced Intrusion Prevention Systems (IPS) that take advantage of behavioral biometrics through deep neural networks. This includes protecting critical infrastructure, where a breach has catastrophic consequences for national stability. Given that malicious insider threats are identifiable [11], incorporating keystroke biometrics in user authentication serves as an essential first line of defense against the unauthorized use of other's passwords. Developing user authentication methods is essential to protect critical infrastructure systems from increasingly sophisticated cyberthreats. Keystroke dynamics, a form of behavioral biometrics, is a reliable mechanism to verify the identity of users by analyzing unique typing patterns.

This chapter presents a complex methodology for enhancing user authentication in critical infrastructure systems using keystroke dynamics and advanced deep learning techniques. The proposed approach addresses the growing need for trusted cybersecurity measures that can effectively detect and prevent unauthorized access, including insider threats.

The methodology introduced in this chapter comprises several key components:

- A novel technique for transforming keystroke dynamics data into image representations, called Gabor Filter Matrix Transformation (GAFMAT) (Section 2.2).
- The application of SNN with CNNs branches for processing the transformed keystroke data (Section 2.3).
- Advanced visualization techniques for analyzing high-dimensional embeddings generated by the neural network (Section 2.4).
- A data fusion approach to standardize keystroke dynamics across different password lengths and datasets (Section 2.5).

This integrated approach aims to improve the accuracy and strength of user authentication by utilizing the unique typing patterns of individuals. The methodology is designed to be adaptable to various critical infrastructure environments and capable of continuous monitoring for anomalous behavior.

The research findings and components of this methodology have been published in several peer-reviewed articles [A.1, A.2, A.3].

2.1. Static Keystroke Dynamics Authentication

The static authentication, based on keystroke dynamics, uses the unique typing patterns (see Subsection 2.2.1) of users when entering a password to verify their identity [117]. This approach improves security by providing an additional layer of verification beyond traditional password-based systems, making them more resistant to unauthorized access, even when passwords are vulnerable. In addition, static keystroke authentication does not require additional hardware, making it cost-effective and seamlessly integrated into existing authentication systems. However, to achieve high accuracy, robust feature extraction and efficient deep learning-based models are required to reduce the false acceptance and rejection rates.

The proposed static authentication in this thesis (see Figure 2.1) utilizes keystroke dynamics to verify the user's identity by analyzing unique typing patterns when entering a password. The system captures timestamps of each keystroke's press and release actions, generating detailed time-series data. These data are then transformed into image representations, enabling efficient comparison of the user's typing behavior against a predefined database. This image is then compared against a pre-established database to ascertain the presence of a similar, previously entered password linked with the username. Access to the system is granted if a corresponding match is identified. Conversely, when no matching password is identified, the IDS generates an informational log, prompting the user to re-enter the password. If the user fails to enter the password correctly after a certain number of attempts defined by group policy, the user's account becomes locked out. This action triggers the IPS, which then generates a critical log. Subsequently, the security operations center specialists are alerted. Hence, even in scenarios where a password within the critical infrastructure is compromised or illegally acquired by an unauthorized person, the system is capable of detecting inconsistencies in the input pattern. This process effectively shows that the current user is not the legitimate owner of the password. Such a mechanism significantly increases the system's resilience to potential security breaches, as demonstrated in [A.2].

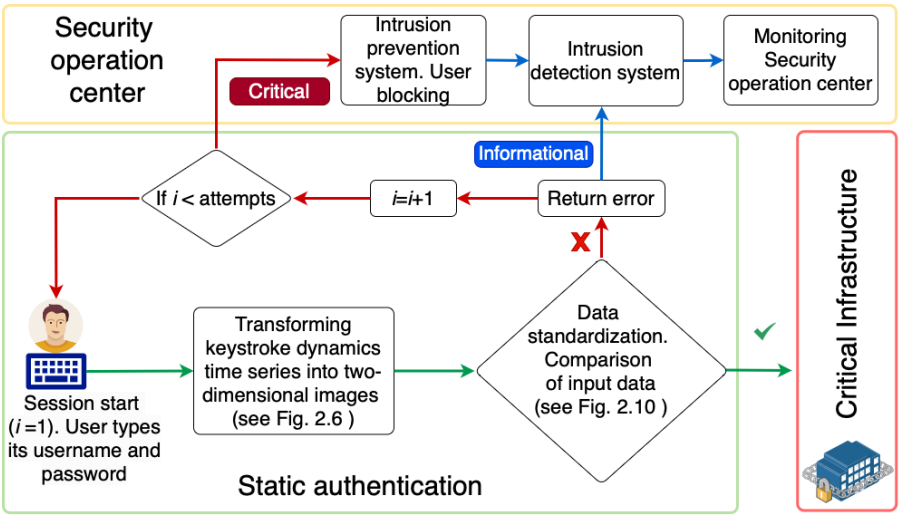


Figure 2.1: Schematic representation of the user authentication process using an intrusion detection system and an intrusion prevention system based on user typing behavior

This approach introduces a significant opportunity to integrate password authentication techniques into critical infrastructure. The challenge lies in discerning the similarity of keystroke dynamics to determine whether the password input was executed by a legitimate user or an insider.

2.2. Non-Image to Image Transformation

Building on the methodology for user authentication described in Section 2.1, this section introduces the extraction of features from keystroke dynamics, discusses existing methods for transforming data into images, and describes a new method proposed in this chapter.

2.2.1. Keystroke Dynamics Datasets

Keystroke biometric models are developed by capturing the time of keystrokes, where the time between each keystroke and the release of the key is recorded. By analyzing these timing information, various features can be extracted. Keystroke biometric models capture temporal characteristics of typing patterns, including:

- Hold time: duration a key is pressed,

- Press-Release time: time between pressing and releasing a key,
- Press-Press time: time between consecutive key presses,
- Release-Release time: time between consecutive key releases.

These features provide very important insights into the typing habits of users, forming the basis for authentication (see Figure 2.2). This method of collecting time series data forms the basis of a comprehensive analysis. Using a machine learning approach, it is possible to extract features of keystroke dynamics. This process provides valuable information on the unique typing patterns of users.

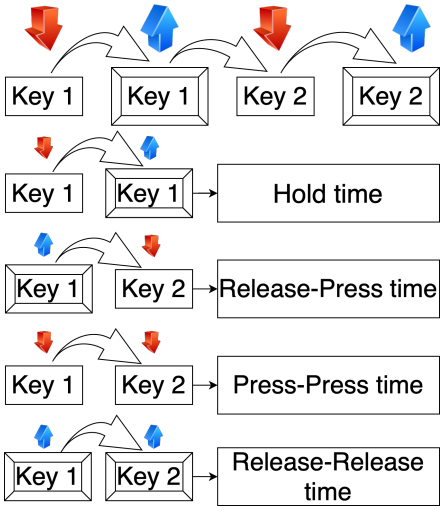


Figure 2.2: Visualizing keystroke dynamics capturing model

These processes have allowed researchers to obtain consistent writing patterns across multiple sessions, creating publicly available fixed-text datasets that are widely used as benchmarks. In this thesis, these datasets will be utilized:

- The CMU dataset [56] consists of 51 participants, each of whom was instructed to enter the password ".tie5Roanl" over eight sessions. The number of timestamps (features) is equal to 31. During each session, participants were required to enter the password 50 times, resulting in a complete dataset of 20,400 password records.

- The KeyRecs dataset [26] consists of 99 participants from all over the world, each performing the "vpwjkeurkb" password task structured dataset into 19,773 samples. The number of timestamps (features) is equal to 46. This dataset not only reflects the diverse keyboard typing patterns of the participants themselves, but also includes demographic information such as age, gender, hand type, and nationality, providing a rich source for analysis.
- The GREYC-NISLAB dataset [41] includes five different passwords entered by 110 users. The passwords are as follows: "leonardo dicaprio", "the rolling stones", "michael schumacher", "red hot chilli peppers", and "united states of america", with the spellings preserved as in the original dataset. In the following text, subsets of data are referred to using the notations LDC, TRS, MS, RHCP, and USA to denote the data corresponding to each specific password. The number of timestamps (features) ranges from 64 to 92. Each participant entered these passwords ten times with both hands and ten times with the dominant hand, yielding 20 samples per user for each password. Thus, the dataset for each password included 2,200 instances, totaling 11,000 data samples for the entire study.

Keystroke biometric models derive key temporal characteristics (e.g. hold times and keystroke intervals) from each keystroke to build a unique profile of user behavior. These features allow the capture of consistent typing patterns over multiple sessions, resulting in publicly available datasets such as CMU, KeyRecs, and GREYC-NISLAB, which are widely used for the research and development of keystroke-based authentication systems. These datasets will be used further in the thesis to evaluate the proposed methodology and user authentication solutions.

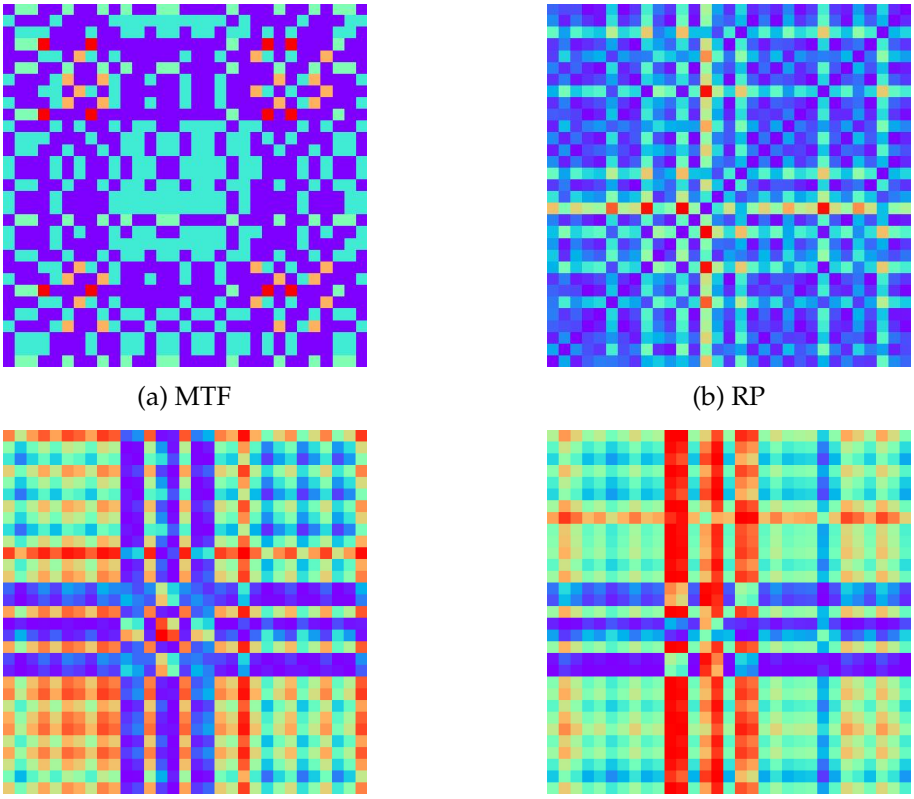
2.2.2. Image-Based Time Series Data

In some applications, it is necessary to transform numerical data into images so that CNNs can effectively extract and analyze features from these images. This transformation allows CNNs to leverage their full mathematical potential by utilizing their powerful feature extraction capabilities, which are inherently designed for image data [24, 35, 119]. By arranging features in a two-dimensional space, the relationships between them can be emphasized, allowing CNN-based models to

extract features that are often outperforming traditional methods that rely only on tabular or numerical inputs. Taking advantage of these feature relationships, CNNs can improve prediction or classification performance compared to models trained solely on tabular data [119]. In the transformation process, each sample of tabular data is converted into an image. In these images, the features and their values are represented by pixels and pixel intensities, respectively.

A number of methods exist for transforming (or encoding) numerical or non-image data into images, such as GASF, GADF, MTF, and the RP methods [25, 107]. These methods are used in various applications, including biometrics for user authentication. The purpose of these transformations is to extract meaningful features from the data, enabling further analysis using deep learning techniques. Each method under review emphasizes specific data characteristics such as frequency, distribution, similarity, amplitude fluctuations, periodicity, or underlying patterns.

Techniques such as GASF, GADF, MTF, and RP can be used to improve the performance of deep learning-based methods for user authentication from biometric data [25, 107]. GASF and GADF, like MTF and RP, are able to capture important time series features, including periodicity, trend, and irregularity. The GASF and GADF methods, which are based on the Gramian Angular Field (GAF) technique, transform time series signals into images by transferring them into polar coordinate space [107]. The GASF method considers the sum of the angles, whereas GADF emphasizes the difference, thereby highlighting distinct aspects of the data. RP is a method for analyzing dynamical systems and time series data. It facilitates the uncovering of the overall structure, non-stationarity, and hidden recurrent elements of a time series. In addition, RP provides a graphical representation of recurrent dynamics. It characterizes the proximity of states in the state space of a dynamical system reconstructed with a time delay [20]. RP is less effective at encoding very long sequences. For very long sequences, the resulting RP images become so large that their discretization is relatively small [114]. In contrast, MTF transforms time series into visual representations. This approach captures significant dynamics and facilitates the use of CNNs to extract and analyze features in various domains [115]. Employing transformation methods in CMU datasets such as GASF,



(a) MTF (b) RP

(c) GASF (d) GADF

Figure 2.3: Example of a typed password of the same user obtained by different methods: a) Markov transition field, b) Recurrence plot, c) Gramian angular summation field, d) Gramian angular difference field

GADF, MTF, and RP, as described in [35], allows the transformation of these individual keystroke dynamics into images. Consequently, this process yields four different images for each method, all representing the same password, as illustrated in Figure 2.3.

These methods represent only a few of the ways in which time series or non-image data can be transformed into images for analysis using deep learning techniques. They demonstrate diverse approaches for transforming time series or non-image data into images suitable for deep learning analysis. The choice of an appropriate method largely depends on the features of the data and the specific problem to be solved. Experimental results comparing and demonstrating the effectiveness of these techniques have been published in [B.2].

2.2.3. GAbor Filter MAtrix Transformation

In the context of behavioral data, such as keystroke dynamics, conventional non-image-to-image transformation methods, including GASF, GADF, MTF, and RP, have been demonstrated to be valuable tools for facilitating CNN-based feature extraction. Nevertheless, these methodologies are not without their limitations, which may impede their efficacy in fully capturing the distinctive typing characteristics that are imperative for user authentication. For instance, GASF and GADF primarily rely on summation and difference of angular values in time series data, which may overlook subtle patterns crucial for distinguishing users. Additionally, RP encounters challenges in effectively encoding very long sequences due to its diminishing resolution as the sequence lengthens. These limitations underscore the necessity for a novel transformation technique that is tailored to behavioral data, one that emphasizes typing patterns in a more comprehensive manner while maintaining compatibility with CNNs for robust feature extraction. The development of such a method could provide more precise and reliable insights into keystroke dynamics, enhancing authentication systems.

Drawing upon insights gained from the analysis of the literature and the transformation of non-image data into images (see Subsection 2.2.2), a new method called GAFMAT (GAbor Filter MAtrix Transformation) was developed by the author of this thesis. This approach is grounded in the principles of the Gabor filter [55]. Keystroke dynamics, which include timing and rhythm variations, are crucial for identifying individual typing patterns. The Gabor filter has high performance in both frequency and time localization, enabling it to capture these variations effectively. It has the capability to isolate specific frequencies while simultaneously retaining information about the timing of events in the signal. The keystroke dynamics data may contain noise due to variations in typing speed, keyboard differences, or environmental factors. The specificity of the Gabor filter provides a natural robustness to such noise:

$$gabor = \exp\left(-\frac{0.5 \cdot x'^2}{\sigma^2}\right) \cdot \cos\left(2\pi \cdot \frac{x'}{\lambda} + \psi\right), \tag{2.1}$$

$$x' = x \cdot \cos\theta,$$

where

- σ: Parameter defining the filter width. A larger σ results in a wider filter.
- θ: Orientation of the filter. In the 1D case, it effectively scales the values of x.
- λ: The wavelength of the sinusoidal factor that determines the frequency of the filter. A larger λ results in a lower frequency filter.
- ψ: This is the phase offset of the sinusoidal factor, which can be used to create bandpass or band-reject Gabor filters.
- x: the numerical value of timestamp of keystroke dynamics.

It filters out irrelevant fluctuations while preserving the essential characteristics of keystroke dynamics [48]. The proposed method, GAFMAT, transforms time series data into image representations. This novel approach shows promising potential for improving the analysis and interpretation of keystroke dynamics in authentication systems. The Gabor filter has been chosen for its specific design for feature extraction in two-dimensional images. The process involves adapting and applying the Gabor filter to one-dimensional time series or discrete signals (2.1), thus emphasizing features of keystroke dynamics (see Figure 2.4). In the figure, there are two curves: the original discrete signal is depicted as a blue line, while the dashed orange line represents the values of the discrete signal after applying the Gabor filter. It is important to note that the Gabor filter, by its nature, highlights features of the discrete signal. As shown in the figure, the filter particularly emphasizes the peaks of the signal. Using the distinctive properties of the Gabor filter, the goal is to improve the representation and visualization of keystroke dynamics. This improvement facilitates more effective discrimination and analysis of key features within time series data.

The *GaborFilter* function (see Algorithm 1) is used to apply a Gabor filter to the timestamps generated by password input. This function takes a discrete signal, representing the timestamps of entered passwords, and several parameters, including σ, θ, λ, and ψ, which define the characteristics of the Gabor filter. The function determines the value of the discrete signal and generates a range of values based on the parameter σ. These values are then transformed using the θ parameter. The Gabor filter is calculated by combining the exponential and cosine

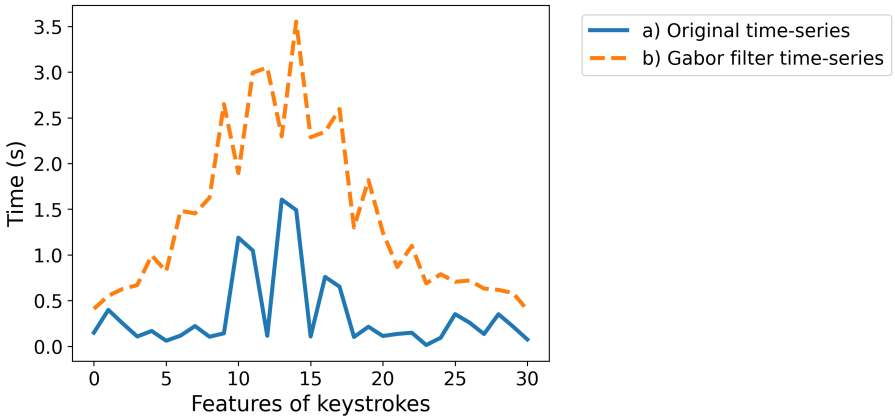


Figure 2.4: Emphasizing the time series features of keystroke dynamics using the Gabor filter: blue for the discrete signal and dashed orange for the discrete signal after applying the Gabor filter

functions based on the provided parameters. The resulting filter is then normalized. Finally, the signal is convolved with the Gabor filter, and the output is returned as a filtered signal (see Algorithm 1).

Algorithm 1 Gabor filter algorithm

function GABORFILTER($discrete\_signal, \sigma, \theta, \lambda, \psi$)
    $length \leftarrow$ length of $discrete\_signal$
    Initialize x as an array of size $length$ generating evenly-spaced values in an interval $(-3\sigma, 3\sigma)$
    $x' \leftarrow x \cdot \cos\theta$
    Initialize $gabor$ as an empty array of size $length$
    $gabor \leftarrow \exp\left(-0.5 \cdot \left(\frac{x'}{\sigma}\right)^2\right) \cdot \cos\left(2\pi \cdot \frac{x'}{\lambda} + \psi\right)$
    $gabor \leftarrow \frac{gabor}{\sqrt{\sum_{i=0}^{length-1} gabor[i]^2}}$
    $gabor \leftarrow Convolution(discrete\_signal, gabor)$
return $gabor$
end function

The GAFMAT algorithm (see Algorithm 2) is specifically designed to create an image representation of a given discrete signal by applying the Gabor filter (see Algorithm 1). The *GaborFilter* function uses a discrete signal and a list of parameters $(\sigma, \theta, \lambda, \psi)$ (see Table 2.1). The algorithm begins by initializing an empty image array that matches the

Table 2.1: List of parameters used for the GAFMAT algorithm

Parameter	Values
σ	2, 4, 8, 16
θ	0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$
λ	16, 8, 4, 2
ψ	0, $\frac{\pi}{4}$, $\frac{\pi}{2}$, $\frac{3\pi}{4}$

shape of the input signal. Then iterates through various combinations of the parameter, applying the *GaborFilter* function to the discrete signal with each iteration. Finally, the algorithm returns the resulting image, which represents the combination of multiple Gabor-filtered versions of the original discrete signal (see Algorithm 2). The outer product of two arrays is computed, producing a new array where each element is the product of the corresponding elements from the input arrays. This computation involves all possible pairwise products of the original time series array and the values obtained by the GAFMAT, which are then systematically arranged in a matrix structure (2.2). The resulting matrix $image2D$ represents the pairwise products of each element in arrays a and b. The matrix $image2D$ is finally visually represented as an image offering a comprehensive visual representation. Such a visualization provides a clear and intuitive understanding of the data, enabling efficient interpretation and analysis of key patterns and relationships (see Figure 2.6).

Algorithm 2 GAFMAT algorithm

Require: $discrete\_signal, \sigma\_list, \theta\_list, \lambda\_list, \psi\_list$
1: $length \leftarrow$ length of $discrete\_signal$
2: $image2D \leftarrow$ create zero array of size $length \times length$
3: $combinations \leftarrow CartesianProduct(\sigma\_list, \theta\_list, \lambda\_list, \psi\_list)$ ▷ The set of all possible parameters (see Table 2.1)
4: **for** each $(\sigma, \theta, \lambda, \psi)$ in $combinations$ **do**
5: $gabortemp \leftarrow GaborFilter(discrete\_signal, \sigma, \theta, \lambda, \psi)$ ▷ see Algorithm 1
6: $gabor \leftarrow transpose(gabortemp)$
7: $image2D \leftarrow image2D + OuterProduct(discrete\_signal, gabor)$
8: **end for**
9: **return** $image2D$

$$image2D = \begin{bmatrix} a_1b_1 & a_1b_2 & \cdots & a_1b_n \\ a_2b_1 & a_2b_2 & \cdots & a_2b_n \\ \vdots & \vdots & \ddots & \vdots \\ a_nb_1 & a_nb_2 & \cdots & a_nb_n \end{bmatrix} \tag{2.2}$$

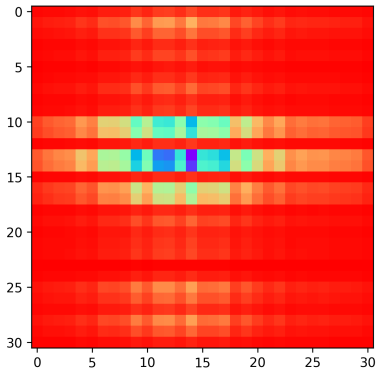


Figure 2.5: The result of transforming the time series features of keystroke dynamics into an image using the GAFMAT algorithm

The newly proposed GAFMAT method enhances the user's keystroke dynamics by scaling up significant values. This scaling results in larger numerical values that are accentuated with a variety of colors. Its robustness to common noise and interference also distinguishes it from traditional approaches.

To summarize the core concept of this method, it can be effectively illustrated using the visual representation in Figure 2.6. When entering a password or passphrase, a sequential dataset is generated that captures each keystroke dynamics timestamp such as hold time, release-press time, press-press time, and release-release time. This time series forms a discrete signal a (as shown in the upper left corner of Figure 2.6), representing the unique rhythm and speed of the user's typing behavior. The next step applies the Gabor filter, which is mathematically expressed and graphically illustrated in the central part of Figure 2.6, and is tuned appropriately to highlight significant features in keystroke data. The idea behind this method, shown in Figure 2.6, is to apply a Gabor filter to the discrete signal obtained from the keystroke dynamics. The Gabor filters, whose parameters are the filter width (σ), orientation (θ), wavelength (λ), and phase offset (ψ), are taken from given values

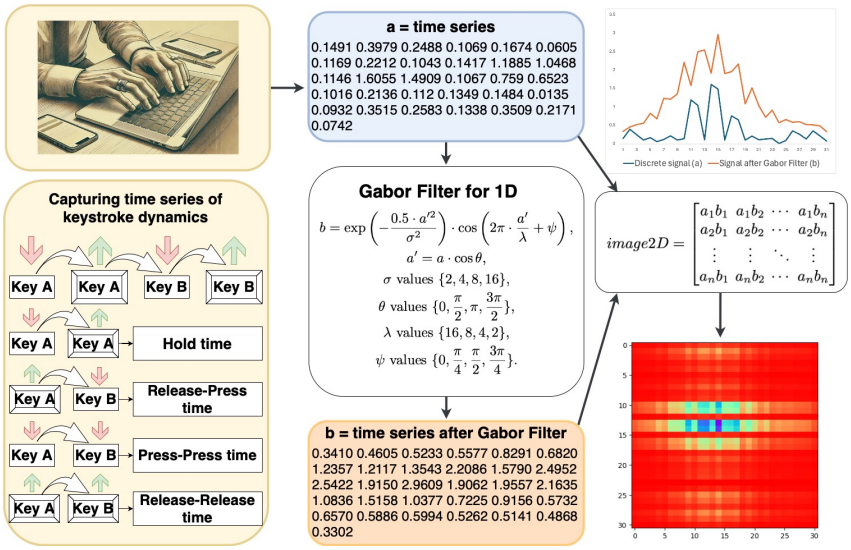


Figure 2.6: The GAFMAT approach for transforming keystroke dynamics time series into two-dimensional images. The process illustrates the application of Gabor filters to emphasize significant features in the data, followed by transforming the filtered data into a two-dimensional image that represents typing behavior. A visual element in the top-left corner is adapted from [32]

to emphasize key features in the data, resulting in the *a* signal being transformed to a *b* signal. Tuning the Gabor filter involves a sequence of operations in which the filter is applied repeatedly, each time with a different set of unique parameters. The Gabor filter extracts certain characteristics from keystroke signals, thus improving the dynamic analysis of keystrokes. As a result of the filters, the *b* signal becomes a transformed series enriched with distinctive features emphasized by applying the Gabor filter.

Subsequently, this filtered time series, together with the original time series of keystroke dynamics, is used to create a two-dimensional image (*image2D* in Figure 2.6) using an outer product operation. This converts a sequence of discrete signals as a time series into a two-dimensional format that can be visually represented. In this case, the variations and patterns in the timing of keystrokes (which are captured sequentially as they occur over time) are translated into an image, where these temporal patterns are represented as variations in color or intensity

patterns over the entire image.

The proposed framework, which is described in this section, the Gabor Filter MAtrix Transformation (GAFMAT) algorithm, as well as the methods and algorithms related to the content of the following section, have been published in [A.2, B.1, B.2] (see the list of author's publication). The result is an image that represents typing behaviors in a visually interpretable format (as shown at the bottom of Figure 2.6). This two-dimensional image not only depicts the complexity of keystroke dynamics as a visual pattern, but also provides a basis for subsequent pattern recognition and deep learning analysis. The framework demonstrates a novel approach to transform keystroke dynamics into a visual representation.

2.3. Siamese Neural Networks Architecture for User Authentication

In 1993, Bromley and colleagues introduced Siamese Neural Networks (SNNs) as a method of solving signature verification tasks. The method involves comparing two input samples to determine their similarity [15]. The network architecture was designed to address problems involving pairwise comparisons, such as verification and authentication, by learning a similarity metric between input pairs. Over time, SNNs have gained significant traction in various fields, including facial recognition, image matching, and biometric authentication, due to their ability to efficiently handle tasks that require comparison between two inputs.

SNN are effective at recognizing and distinguishing between different typing patterns. Transforming keystroke dynamics data into images (see Section 2.2) takes advantage of the proven mathematical ability of CNNs to extract sophisticated features. This network effectively uses filters of varying sizes to capture and analyze data at different spatial resolutions, thereby enhancing the system's ability to learn and recognize typing patterns efficiently. This approach exploits the strengths of CNNs, allowing the development of more accurate and reliable user authentication systems based on unique typing behavior.

The SNN architecture uses three CNNs branches and a triplet loss function at the output layer. This setup estimates the distance between the images as detailed in [15, 89] (see Figure 2.7). More recently, training SNN frequently involves using triplets composed of an anchor, a

positive, and a negative sample:

- anchor (A) – a reference sample against which other items are compared,
- positive (P) – a sample that is similar or related to the anchor,
- negative (N) – a sample that is not similar or related to the anchor.

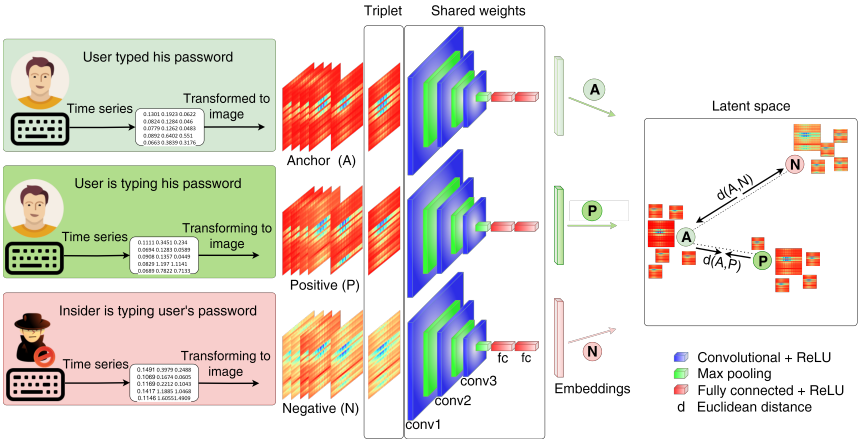


Figure 2.7: Schematic representation of the proposed framework for time series transformation from keystroke biometric data features into images and the training process of SNN with CNNs branches

During the network training process, triplets are formed. These triplets consist of an anchor image, a positive image from the same user, and a negative image from another user. After training, SNN creates corresponding embeddings for all triplets. These embeddings are vectors in a multidimensional latent space that represent the input data or images. The idea is that similar images will produce embeddings located close to each other in this space, while dissimilar images result in embeddings that are more distant (see Figure 2.8). To determine the similarity between two images, the distance between their embeddings can be computed using metrics such as the Euclidean distance or cosine similarity.

In the context of triplets, the distance between the anchor and the positive sample in a multidimensional latent space should be small, indicating high similarity. The distance between the anchor and the negative sample should be significant, indicating low similarity. By

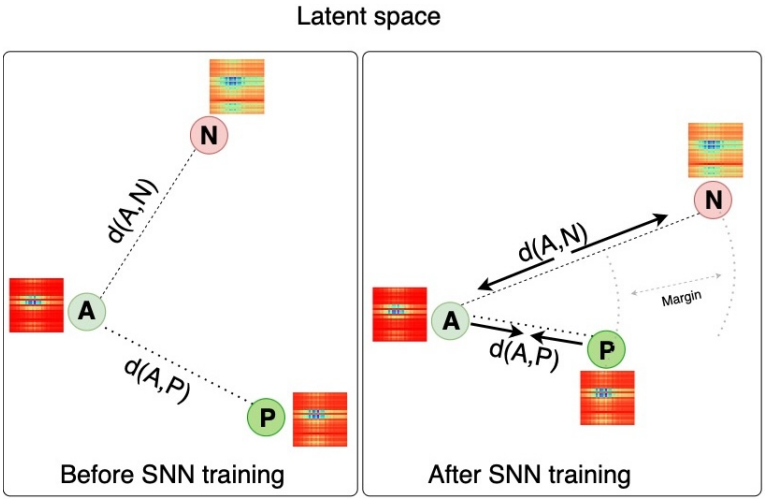


Figure 2.8: Triplet example before and after training SNNs: the triplet loss function minimises and maximises the corresponding distances during network training

exploring these distances, decisions can be made about the similarity or dissimilarity of new, unidentified images (or samples) compared to known anchors.

SNN training process involves looking for similarities between the positive and anchor images while promoting dissimilarities between the anchor and negative samples. The triplet loss function (2.3) is designed to minimize the distance between the anchor and the positive image (as they belong to the same class) while maximizing the distance between the anchor and the negative image (as they belong to different classes) depending on the margin size (see Figure 2.8).

$$L(A, P, N) = \max\left(||f(A) - f(P)||^2 - ||f(A) - f(N)||^2 + \alpha, 0\right), \quad (2.3)$$

where

- $||f(A) - f(P)||^2$ is the squared Euclidean distance between the embeddings of the anchor and positive samples computed in a multidimensional latent space,
- $||f(A) - f(N)||^2$ is the squared Euclidean distance between the embeddings of the anchor and negative samples computed in a

multidimensional latent space,

- f is the embedding function that maps an input to its embedding,
- α is the margin that is enforced between positive and negative pairs.

Numerous researchers have previously used a triplet loss function to train their models, considering it a suitable option for user authentication [21, 28, 29, 88, 111]. The triplet loss function includes a margin that sets the desired separation between positive and negative samples relative to the anchor. The margin size within the triplet loss function was selected based on findings from previous author's publications [B.1, B.2].

The margin within the triplet loss function allows a clear distinction between similar and dissimilar samples, ensuring that the distance or dissimilarity between the anchor and the negative sample is greater than the distance between the anchor and the positive sample by at least a predefined threshold value. During SNN training, enlarging the margin size can affect the Euclidean distance between the anchor and positive images and the anchor and negative images. Nevertheless, a larger margin provides the network with more room to distinguish between positive and negative images relative to the anchor, which can result in improved accuracy. Increasing the margin makes it easier for the network to differentiate between image samples, but it also means that the network has to learn fewer subtle differences, potentially leading to decreased accuracy [B.1, B.2]. Accuracy in this context refers to the ability of SNN to correctly predict the outcome of the validation data. It measures the proportion of correct predictions made by the model and provides an indication of how well the network is able to distinguish between positive and negative images. It is determined by dividing the number of correct predictions made by the model by the total number of predictions.

The choice of the optimal margin is therefore a balance between the dissimilarity of the negative and anchor images and the similarity of the positive and anchor images, and the accuracy of the network. Experimentation may be necessary to find the optimal margin value for a given dataset and task.

Increasing the size of the margin increases the difference between the Euclidean distance between the negative and anchor images and the Euclidean distance of the positive and anchor images, so the network would be more stringent in determining the relationship between the inputs. Thus, the network's ability to accurately recognize the connections between inputs may be hindered, resulting in a decrease in its accuracy.

While SNNs with CNNs branches perform well in image comparison tasks [71, 102, 109], their direct applicability for password keystroke patterns can be challenging due to inherent differences in data structures. By transforming keystroke dynamics into images for CNN training, which is a branch of SNN, this approach takes advantage of the strengths of these networks [92, 119]. This transformation enhances the network's ability to distinguish certain behavioral biometric differences between authentic users and insider typing patterns.

Table 2.2: Summary of CNN used in SNN architecture

Layer (Type)	**Output Shape**	**Number of Parameters**
InputLayer	(None, 31, 31, 3)	0
Conv2D	(None, 31, 31, 128)	24,704
BatchNormalization	(None, 31, 31, 128)	512
MaxPooling2D	(None, 15, 15, 128)	0
Conv2D	(None, 15, 15, 128)	589,952
BatchNormalization	(None, 15, 15, 128)	512
MaxPooling2D	(None, 7, 7, 128)	0
Conv2D	(None, 7, 7, 128)	262,272
BatchNormalization	(None, 7, 7, 128)	512
MaxPooling2D	(None, 3, 3, 128)	0
Flatten	(None, 1152)	0
Dense	(None, 512)	590,336
Dense	(None, 256)	131,328
Lambda	(None, 256)	0

The choice of SNN combined with CNNs branches was based on their effectiveness in image recognition tasks, as they are able to learn similarity measures between input data [A.2, A.3, B.2]. Traditional classification networks may struggle with significant class imbalance, while SNNs may be more robust in such scenarios. Instead of classifying a large number of classes, they measure the similarity to a reference

(anchor). SNNs generalize well to new data. Once trained, they can compare any new sample to a known reference without the need for retraining. The parameters of SNN with CNNs branches were determined by an extensive grid search, evaluating different configurations to achieve the best authentication. A summary of CNN used for SNNs, with an input image size of 31x31, is provided in Table 2.2. The size was determined on the basis of the features of the CMU dataset. Each convolutional layer is followed by batch normalization and max pooling operations. This is followed by a flattened layer, the output of which is used as the input to the dense layer. The last layer of the network has 256 outputs that have been normalized using L2 normalization. The network output can be considered as an embedding of the original input. The network, which has a depth of 12 layers, covers a total of 1,600,128 parameters.

Using SNN architecture [15, 89], the effectiveness of IDS and IPS can be improved by better identifying the user by their unique password input patterns. Consider a given scenario where each password entry is transformed into an image and stored in a database associated with the corresponding username. The system, based on an SNN, is designed to analyze and capture the unique typing characteristics of a user as he or she interacts with the system using a keyboard. This network processes input data to identify and differentiate individual typing patterns. The behavioral data are then aggregated using complex algorithms to create a multidimensional representation in the latent space. This results in individual clusters, each corresponding to a different user. These clusters allow for a detailed study of each user's typing behavior. Each individual possesses a distinct typing style, which makes us unique in the way we interact with the keyboard. If unauthorized access occurs or credentials are compromised, the proposed methodology can identify and prevent unauthorized individuals from exploiting stolen or purchased passwords to gain access to the system. By leveraging the inherent uniqueness of typing patterns, this approach can effectively detect and mitigate unauthorized login attempts. This increases the security and protection of user credentials in the system [A.2, A.3, B.2].

2.4. Data Visualization Techniques for Keystroke Dynamics

In the rapidly growing field of artificial intelligence, deep learning models, widely used in pattern recognition tasks, are excellent at extracting multidimensional features from raw data and transforming them into embeddings that reflect the complex patterns and relationships inherent in the dataset. However, the multidimensional nature of these embeddings presents a major challenge: they cannot be easily interpreted by humans without additional analysis. This comprehensibility gap requires effective dimensionality reduction and data visualization strategies, which are important for several reasons. Dimensionality reduction is crucial to overcome the "curse of dimensionality", a phenomenon in which a high-dimensional feature space leads to a sparse data distribution. As the dimension increases, the volume of the space increases exponentially, making the available data too sparse to produce reliable results. This sparsity makes it difficult for algorithms to detect patterns or make predictions with high accuracy. Dimensionality reduction techniques help to overcome this curse and improve the performance and accuracy of machine learning models.

In the context of keystroke dynamics for user authentication, it is often necessary to deal with multidimensional data. Each keystroke event generates multiple features such as keystroke duration, delay between keystrokes, and typing rhythm. To analyze this complex data, this thesis uses SNN with a triplet loss function. This network processes keystroke data and creates multidimensional embeddings that reflect unique characteristics of the user's typing behavior. However, these embeddings, typically located in a space of 256 or more dimensions, are not directly interpretable. This is where visualization techniques can provide invaluable assistance. This visualization not only validates the network's ability to distinguish between users, but also provides an intuitive way to evaluate system performance and reliability. Combining neural network architectures with known visualization techniques allows for a visual representation of the information obtained and improves interpretability.

Visualization techniques are crucial in cybersecurity, particularly for Security Operations Centers (SOC), as they enable analysts to quickly identify and respond to security threats by transforming complex data

into clear and actionable insights. This subsection presents a proposed dimensionality reduction-based visualization framework for multidimensional embeddings derived from deep neural networks to improve decision-making for better data comprehension in solving complex problems where similarities and dissimilarities between data samples need to be revealed. The transformation of non-image into images is described. Dimensionality reduction-based visualization of the multidimensional embeddings obtained by a Siamese neural network with triplet loss function is discussed.

During the training process, triplet samples are formed, consisting of an anchor image, a positive image from the same user, and a negative image from a different user. After training, the network generates embeddings that map these samples to a multidimensional latent space. In this space, the proximity of embeddings signifies similarity, where similar samples (anchor and positive) are clustered closely, while dissimilar samples (anchor and negative) are farther apart. Visualization of these embeddings is crucial as it allows for a deeper understanding of the network's ability to differentiate between users. By visualizing the spatial relationships between embeddings, researchers can assess how well the model distinguishes similar from dissimilar inputs, aiding in the assessment of authentication accuracy. This is often achieved using distance metrics like Euclidean distance or cosine similarity, which quantify the relative closeness of the embeddings. Through such visual representations, it is possible to evaluate and refine the model's performance in identifying patterns in user behavior.

In solving the dimensionality reduction problem, a final transformation is sought that maps multidimensional embeddings $E_i \in \mathbb{R}^p$ to a set of points $Y_i = (y_{i1}, \ldots, y_{id})$, where $i = 1, \ldots, m$ and $d < p$, in a lower-dimensional space. This process is very important for interpreting embeddings, as it transforms complex keystroke patterns into a more convenient and visually interpretable format. By setting $d \leqslant 3$, a graphical representation of the data becomes possible, which is very important for decision support, in this case, for user authentication. Visualizing these reduced embeddings in two or three dimensions provides an intuitive view of the underlying structures and variations in keystroke dynamics, thus helping to identify genuine users and potentially illegitimate users.

This section introduce exploration of visualization techniques tailored for cybersecurity, particularly focusing on their utility within security operations centers. By implementing a dimensionality reduction-based framework, the thesis enhances the interpretability of complex, multidimensional embeddings derived from SNN with CNNs branches, facilitating improved decision-making processes. The core of this methodology is the transformation of keystroke dynamics into visually interpretable formats. This approach not only simplifies the visualization of embeddings to highlight similarities and differences effectively but also supports the authentication accuracy through precise visual analysis of data relationships using common distance metrics. The detailed visualization framework outlined demonstrates each step from data preprocessing to the final decision support, emphasizing the enhancement of data comprehension in cybersecurity operations and providing a robust platform for security analysts to detect and respond to threats efficiently.

2.5. Keystroke Dynamics Data Fusion-Based Methodology for User Authentication

Behavioral biometrics, especially keystroke dynamics, collects time series data, and each password or passphrase entered has a unique set of features. In the case of time series analysis, fusing different datasets into a single dataset is a challenging task that can be addressed by a variety of approaches. Interpolation techniques are particularly effective in standardizing datasets of different lengths to make them more uniform for analysis.

2.5.1. Data Fusion-Based Authentication

Statistical or machine learning-based methods, such as cubic, linear [42], nearest neighbor [96], resampling, Dynamic Time Warping (DTW) [74], and Fourier transform, can be used to unify time series of different lengths. These methods can be used to standardize datasets and thus facilitate the application of complex analytical models. When a network is trained on the fused dataset, its generalizability is enhanced, allowing it to perform more effectively across different types of data in real-world scenarios. DTW is an efficient method for aligning sequences that

differ in speed or time; it requires significant computational resources and is less appropriate for larger datasets. This is because the process of determining the alignment of two time series is complex (typically $O(lenght1 \times length2)$, where $length1$ and $length2$ are the lengths of the two sequences being compared). The Fourier transform is less efficient than simpler interpolation methods, especially for large datasets or applications that require real-time processing. In contrast, interpolation methods such as linear, cubic, and nearest neighbor methods are much less computationally intensive. Each interpolation method has its own advantages and limitations, so the choice of method depends on the specific characteristics of the data to be analyzed and the desired result of the interpolation process.

The author's publications [A.2, A.3] proposes a new keystroke dynamics-based authentication approach, focusing on data fusion from multiple datasets to improve existing methodologies. Previous studies (see Section 1.3 and 1.4) have predominantly relied on a single dataset for training and evaluation, which restricts the model's ability to generalize across diverse user populations and typing behaviors. This research addresses that limitation by utilizing data fusion techniques, allowing the deep learning model to process more varied input patterns and better adapt to the variability present in real-world authentication scenarios. By combining multiple datasets, the system can learn a more generalized and robust representation of keystroke patterns, enhancing its performance in practical applications. This method, involving the selection of appropriate interpolation techniques and the fusion of complex keystroke dynamics data, advances the existing body of work on keystroke biometrics by increasing the model's resilience to environmental and behavioral inconsistencies.

It is imperative to incorporate an effective user authentication methodology into critical infrastructure systems, which necessitates accounting for the considerable variability in the length of passwords utilized by individuals. Instead of training a distinct neural network for each user, an optimal solution would entail the development of a single neural network capable of recognizing and distinguishing between the passwords of all users. This would facilitate the process by enabling the model to generalize across diverse user inputs, thereby providing scalability and reducing the necessity for repetitive training. By training

the network on a single password, the system could be extended to accommodate multiple users, thereby providing a flexible cybersecurity solution. Furthermore, a significant advancement in this methodology is the fusion of multiple datasets, which enhances the learning capability of the deep learning model. The process of data fusion enables the model to more effectively adapt to the inherent variability present in real-world scenarios, thereby ensuring its resilience against the emergence of diverse and evolving authentication patterns. This approach enhances the model's generalization ability, rendering it well-suited for the dynamic and complex requirements of cybersecurity in critical infrastructures.

The data fusion-based authentication framework utilizing complex keystroke dynamics involves two steps: determining a suitable interpolation method (see Figure 2.9) and implementing data fusion-based authentication using complex keystroke dynamics (see Figure 2.10).

The flowchart in Figure 2.9 illustrates the methodology for selecting the most appropriate interpolation method to unify keystroke dynamics data from different datasets. Three interpolation methods (linear, cubic, and nearest neighbor) are first applied to the original time series to standardize the number of features of each password (see the left side of Figure 2.9). After these interpolation processes, the GAFMAT approach (see Subsection 2.2.3) is used to transform the output into images, effectively converting passwords of different lengths into images of the same dimensions. Another possible way to unify the dimensions of the data is to first transform the time series corresponding to the passwords into images using the GAFMAT method, and then unify the size of the resulting images using interpolation techniques such as bilinear, bicubic, and nearest neighbor methods (see the right side of Figure 2.9). Regardless of which data standardization solution is used, the resulting images are used to form triplets—groups consisting of an anchor, a positive sample from the same user, and a negative sample from another user. These triplets are used to train an SNN to distinguish the typing behavior of the keystroke dynamics of the users.

The trained network embeds the data in a multidimensional space, where the distances between anchor-positive and anchor-negative pairs are analyzed. The goal of the model is to minimize the distance between similar pairs (anchor and positive) and maximize the distance between

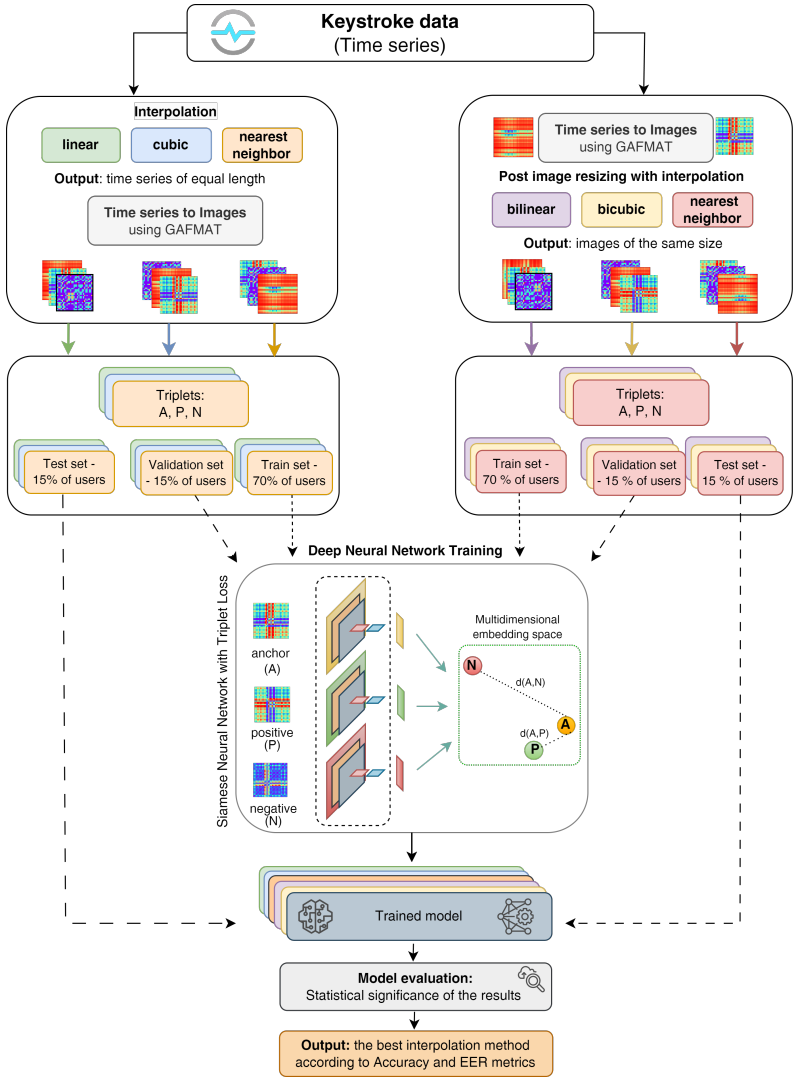


Figure 2.9: Flowchart for selecting the most appropriate interpolation method for data fusion to unify keystroke dynamics data from multiple datasets: the decision-making process for applying interpolation methods to either original time series data or images transformed using the GAFMAT approach, resulting in a unified data format for Siamese neural network training

dissimilar pairs (anchor and negative). After training, the model is evaluated by examining the accuracy and EER. Therefore, based on accuracy and EER, the best interpolation method is determined that best standardizes the keystroke dynamics data for the deep learning model.

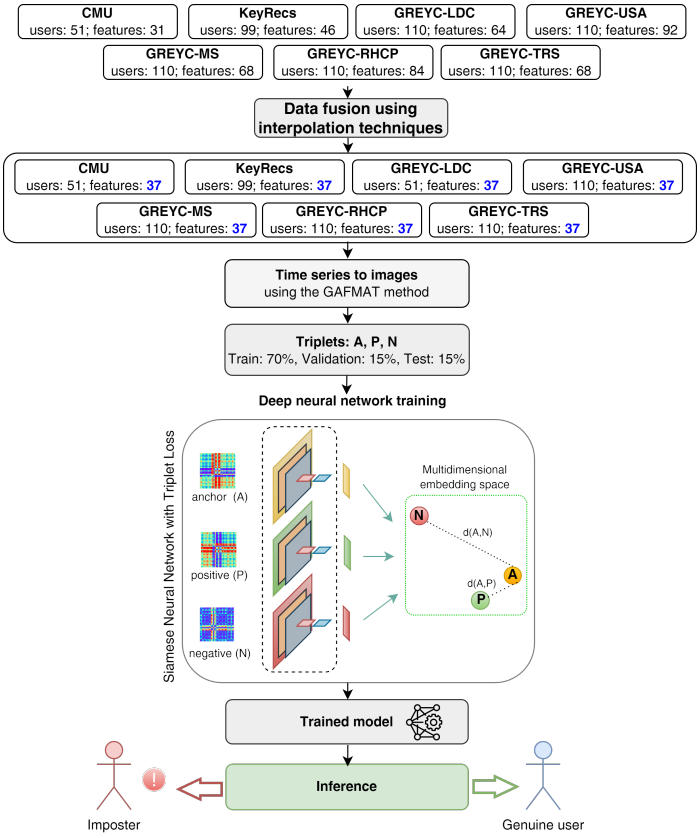


Figure 2.10: A solution for data fusion-based authentication using complex keystroke dynamics analysis. It includes steps for standardizing datasets through interpolation, transforming password samples into images, and using a trained SNN to compare embeddings of new inputs with stored records for user authentication

The methodology presented in Figure 2.10 is designed to authenticate users by analyzing the unique characteristics of keystroke dynamics. It establishes a systematic approach for fusing all passwords for user identification. Initially, the CMU, KeyRecs, and GREYC-NISLAB (LDC, MS, RHCP, TRS, USA) datasets, which vary in the number of users and features, are standardized by interpolating to a single number of features to ensure uniformity before further processing. Details on the datasets are provided in Subsection 2.2.1. By fusing data from multiple datasets into a unified size, the approach ensures consistent input data for an SNN, allowing the model to be trained on a diverse set of user input patterns. In the inference phase, the user provides a sample of

his/her password, which is then transformed into an image. The trained network processes this image and generates an embedding, the vector representation of the image in multidimensional space. The embedding is then compared to the embeddings of previously stored password images of the same user. The distance between the embeddings in multidimensional space is computed for this comparison. A very important part of this methodology is the establishment of a threshold to distinguish between genuine and insider attempts. This threshold is initially determined from the historical data of legitimate logins, taking into account the distance range found in the embeddings of real password records. An attempt is considered genuine if the distance does not exceed a specified threshold; otherwise, it is considered an insider.

2.5.2. Interpolation-Based Data Fusion

Commonly, SNNs, like other neural networks, are trained on a single dataset, which is limited by the unique feature size. In the context of user authentication based on keystroke dynamics, passwords collected from different datasets may exhibit different lengths. When combining password datasets of different lengths, a method is needed to ensure that the format of the data fed into SNN is uniform. In this thesis on keystroke dynamics for user authentication, the analyzed data are time series in which each point is a timestamp. These timestamps reflect the unique rhythm and timing of typing, which are key factors in authenticating a user's identity. In this analysis, "features" specifically refer to the timestamps associated with each keystroke, providing a detailed temporal pattern of password entry. These detailed temporal features are essential for distinguishing between individual users, which improves the accuracy of the authentication process.

Given that an SNN requires a constant size of input data, it is essential to standardize the length of the time series (the number of features) across different datasets. For interpolating time series data, three common interpolation methods can be applied:

- In linear interpolation, new data points in a discrete set of known data points (timestamps) are generated by assuming a straight-line progression between points. This method calculates intermediate values by connecting each pair of adjacent data points with a

straight line, effectively standardizing the length of the time series by filling in or expanding the data to a uniform scale.

- In cubic interpolation, a smoother and more continuous curve is constructed through known data points using the values of neighboring points. This approach, in which a cubic polynomial is placed between each pair of data points, provides a greater degree of smoothness and accuracy than linear interpolation, resulting in a more accurate representation of the original time series.

- Nearest neighbor interpolation assigns the value of the nearest data point to any new data point, effectively preserving the characteristics of the original dataset.

An alternative approach for standardizing data dimensions involves resizing images using various interpolation methods:

- The bilinear method, which is a two-dimensional extension of linear interpolation, averages the nearest 2x2 grid of pixels, balancing efficiency and image quality with moderate scaling.

- The bicubic method, a more complex method, uses a 4x4 nearest pixel grid and cubic polynomials for a smoother transition, resulting in higher quality images that are ideal for significant resizing.

- The nearest neighbor method, which is the simplest and fastest, directly assigns the nearest pixel value to each new pixel and preserves the original characteristics of the images.

The National Institute of Standards and Technology (NIST) guidelines [44], the leading standard for password security, emphasize that password length contributes more to security than does complexity. The NIST recommends a minimum of eight characters but emphasizes the benefits of longer passwords for increased security. According to the National Cyber Security Centre (NCSC) cyber essentials requirements for IT infrastructure [79], effective password management should include implementing multi-factor authentication or setting a minimum password length. In particular, a minimum password length of at least 12 characters is recommended without a maximum limit.

The keystroke dynamics analyzes not only the characters themselves but also detailed temporal data to provide multiple features for each character. In this thesis, seven different passwords were analyzed, each with an initial number of features ranging from 31 to 92. Consistent with cybersecurity recommendations for a minimum password length of 12 characters, the number of features was standardized to 37 for all data by interpolation. The number of features consists of the hold time, release-press time, press-press time, and release-release time of the keystrokes (for more details, see Subsection 2.2.1). This standardization involved adjusting the number of features of each password, increasing for some and decreasing for others, to a consistent value of 37, thus organizing the data for processing by the same neural network model.

The creation of a comprehensive and resilient user authentication strategy for mission-critical infrastructure systems requires a comprehensive analysis of password length variability and user behavior patterns. Instead of training individual neural networks for each user, a more efficient approach would be to develop a single neural network capable of recognizing passwords for all users. Such an approach would enhance scalability by allowing the model to generalize across various user inputs without the necessity for repetitive training. A significant advancement in this methodology is the incorporation of data fusion techniques, which integrate multiple datasets to create a more comprehensive learning environment for the deep learning model. Data fusion enables the model to better accommodate the variability and unpredictability inherent to authentications in the real world, thereby enhancing its resilience and efficacy in distinguishing between legitimate users and potential threats. By focusing on keystroke dynamics and unifying the data through interpolation techniques, this methodology enhances the overall precision and robustness of the authentication process, particularly in high-security environments.

2.6. Conclusions of the Chapter

The authentication methodology presented in this chapter establishes keystroke dynamics as a viable and hardware-independent solution for securing critical infrastructure systems. SNN with CNNs branches is used to effectively extract keystroke pattern features from time-series data transformed into an image. This transformation allows the model

to exploit the structure of time series data. In particular, the integration of GAFMAT significantly enhances the feature extraction capabilities and overcomes the limitations of existing transformation methods such as GASF, GADF, MTF and RP.

In addition, the use of data fusion and interpolation techniques ensures adaptability to different dataset lengths, facilitating model generalization to different password lengths. The proposed framework demonstrates the need to combine behavioral biometrics, data transformation, and deep learning architecture to create a scalable authentication system that adapts to any length of password for real-world applications.

3. EXPERIMENTS AND RESULTS

This chapter presents a comprehensive evaluation of the proposed user authentication methodology through extensive experimental studies on several datasets. The experiments aim to verify the effectiveness and capabilities of GAFMAT compared to traditional methods. A section utilizing fixed-text datasets from CMU, GREYC-NISLAB, and KeyRecs will demonstrate methodological advancements in user authentication through the approach of SNN with CNNs branches, using the GAFMAT method for data transformation. The main experimental results that are further discussed in this chapter have been published in peer-reviewed journals and conference proceedings (see [A.1, A.2, A.3, B.2]).

The chapter is structured as follows:

- The experimental setup involved training and evaluating the proposed methodology (Section 3.1)
- Performance metrics for keystroke dynamics evaluation (Section 3.2). The key performance metrics used to evaluate keystroke dynamics-based authentication results are presented, focusing on EER.
- CMU dataset experiments (Section 3.3). This section presents detailed results of applying GAFMAT and other transformation methods (GADF, GASF, RP, MTF) to the CMU dataset. The performance of SNN with CNNs branches using these different image representations is analysed.
- GREYC-NISLAB dataset experiments (Section 3.4). An extended evaluation on the GREYC-NISLAB dataset is conducted, demonstrating the adaptability of the GAFMAT method for transforming data into images to different password lengths and complexities.
- Overview of results from CMU and GREYC-NISLAB datasets (Section 3.5). A comparison of the results obtained using the GAFMAT method with traditional methods on both datasets is discussed.
- Keystroke dynamics data visualization (Section 3.6). This section discusses the use of dimensionality reduction techniques to visualize the high dimensional embeddings created by the SNN model used, providing insight into the decision making process.

- Keystroke dynamics data fusion-based experiments (Section 3.7). The results obtained from the application of the proposed methodology using data fusion are presented, demonstrating the generalization of the models using different datasets (CMU, KeyRecs, GREYC-NISLAB).

3.1. Experimental Setup

Table 3.1: Experimental platform technical specifications and system configuration

Platform	**Details**
Model	Apple MacBook Pro 14-inch
Processor Model	Apple M1 Pro
CPU	10-core
GPU	16-core
RAM	32 GB unified
Disk Space	512 GB SSD
Operating System	macOS Sonoma
Python Framework	TensorFlow 2.9.1, Matplotlib 3.7.0, Numpy 1.22.4, Pandas 1.5.3.

To demonstrate the distinctive features and effectiveness of the methodology, experiments were conducted using two publicly available fixed-text datasets: the CMU dataset and the GREYC-NISLAB dataset. The experiments for this thesis were conducted on an Apple MacBook Pro with an M1 Pro chip, featuring a 10-core CPU and a 16-core GPU. Each core is split into 16 execution units (EUs), and each EU consists of 8 arithmetic logic units (ALUs), for a total of 256 EUs and 2,048 ALUs across the GPU. This powerful setup, equipped with 32 GB of unified RAM, ensures the efficient handling of complex computational processes essential for deep learning-based networks, as detailed in Table 3.1. The software environment included TensorFlow [1], a widely used library for machine learning, which allows for optimized CPU/GPU utilization for scalable training and evaluation.

Keystroke dynamics data were transformed into image formats using GAFMAT alongside other comparative methods such as GASF,

GADF, MTF, and RP (see Subsection 2.2.2). These transformations were computed for each dataset to assess their contribution to model performance.

To evaluate the proposed methodology, experiments utilized three publicly available fixed-text datasets (see Subsection 2.2.1): CMU dataset, comprising 51 participants who entered the password ".tie5Roanl" over eight sessions, totaling 20,400 password records; GREYC-NISLAB dataset, characterized by 5 unique passwords typed by 110 users, resulting in 11,000 samples across all passwords; KeyRecs dataset, including 99 participants and 19,773 samples with diverse demographic information such as age, gender, and dominant hand.

3.2. Performance Metrics for Keystroke Dynamics Evaluation

Choosing the right metric is critical to evaluate the performance of SNN-based models. These metrics assess the accuracy of the model in distinguishing between legitimate and unauthorized users, which is very important to ensure system performance in a dynamic cybersecurity environment. For the analysis, each metric was calculated for each batch. The validation dataset represents 30% of the total dataset. Subsequently, each metric was evaluated for each individual batch, and the average value across all batches was reported as the final result. This approach ensured that the metrics were representative of the overall performance of the validation dataset while considering the inherent variability between batches. A comprehensive set of metrics was employed to assess the performance of the trained models, including the following:

- EER, the most commonly used accuracy metric in biometric authentication systems (see Table 1.1) (3.2)
- Area Under the ROC Curve (AUC) (3.3)
- Euclidean distance:
  - Between the embeddings of the anchor and positive samples in a multidimensional latent space (AP_ED)
  - Between the embeddings of the anchor and negative samples in a multidimensional latent space (AN_ED)

- Standard deviation of Euclidean distances:
  - Between the embeddings of the anchor and positive samples in a multidimensional latent space (AP_STD)
  - Between the embeddings of the anchor and negative samples in a multidimensional latent space (AN_STD)
- Cosine similarity (3.4):
  - Between the embeddings of the anchor and positive samples in a multidimensional latent space (AP_CS)
  - Between the embeddings of the anchor and negative samples in a multidimensional latent space (AN_CS)
- Accuracy (3.5)

In evaluating the performance of the proposed methodology, special attention was focused on EER (3.2) as the main metric. EER was chosen due to its wide acceptance and use in biometric authentication systems as a balanced measure of accuracy. EER is a specific point on the ROC curve. It is a rate at which FAR and FRR are equal, offering a simple and effective measure of a system's performance in distinguishing between authorized users and impostors. In the experiments conducted, the accuracy metric for both the validation and test datasets is adapted for the classification task using SNN. This metric determines the fraction of cases where a positive score outperforms a negative score, as shown in (3.5). The positive score represents the Euclidean distance between the anchor embeddings and positive samples in a multidimensional latent space. The negative score corresponds to the Euclidean distance between the embeddings of the anchor and negative samples in the same multidimensional latent space.

$$thr^* \;=\; \arg\min_{thr} \big|\mathrm{FAR}(thr) \;-\; \mathrm{FRR}(thr)\big|, \tag{3.1}$$

$$\mathrm{EER} \;=\; \begin{cases} \mathrm{FAR}(thr^*), & \text{if } \mathrm{FAR}(thr^*) = \mathrm{FRR}(thr^*), \\ \dfrac{\mathrm{FAR}(thr^*) \;+\; \mathrm{FRR}(thr^*)}{2}, & \text{otherwise.} \end{cases} \tag{3.2}$$

- EER: EER — a single scalar value that quantifies the crossover point where FAR and FRR are either equal or as close as possible. If $\mathrm{FAR}(thr^*) = \mathrm{FRR}(thr^*)$ exactly, then $\mathrm{EER} = \mathrm{FAR}(thr^*) = \mathrm{FRR}(thr^*)$. Otherwise, a common convention is to average the two values at thr^*.
- $\mathrm{FAR}(thr)$ is the False Acceptance Rate at a given threshold *thr*, indicating the fraction of impostors incorrectly accepted.
- $\mathrm{FRR}(thr)$ is the False Rejection Rate at a given threshold *thr*, indicating the fraction of genuine incorrectly rejected.
- *thr* is the decision boundary at which FAR and FRR are computed. A real-valued decision threshold used to distinguish between genuine and impostor samples.
- thr^* is the optimal threshold that minimizes the absolute difference between $\mathrm{FAR}(thr)$ and $\mathrm{FRR}(thr)$.

$$\mathrm{AUC} = \frac{1}{N_{\mathrm{pos}} \cdot N_{\mathrm{neg}}} \sum_{i=1}^{N_{\mathrm{pos}}} \sum_{j=1}^{N_{\mathrm{neg}}} I(\mathrm{score}_{\mathrm{pos},i} > \mathrm{score}_{\mathrm{neg},j}), \tag{3.3}$$

where

- N_{pos} is the number of positive samples,
- N_{neg} is the number of negative samples,
- $\mathrm{score}_{\mathrm{pos},i}$ represents the score assigned to the i-th positive sample,
- $\mathrm{score}_{\mathrm{neg},j}$ represents the score assigned to the j-th negative sample,
- $I(\mathrm{score}_{\mathrm{pos},i} > \mathrm{score}_{\mathrm{neg},j})$ is an indicator function that returns 1 if $\mathrm{score}_{\mathrm{pos},i} > \mathrm{score}_{\mathrm{neg},j}$, and 0 otherwise,
- $\sum_{i=1}^{N_{\mathrm{pos}}} \sum_{j=1}^{N_{\mathrm{neg}}} I(\mathrm{score}_{\mathrm{pos},i} > \mathrm{score}_{\mathrm{neg},j})$ counts the number of correctly ranked pairs of positive and negative samples,
- AUC measures the probability that a randomly chosen positive sample is ranked higher than a randomly chosen negative sample.

$$\text{CosineSimilarity}(x, y) = \frac{\sum_{i=1}^{n} x_i y_i}{\sqrt{\sum_{i=1}^{n} x_i^2} \cdot \sqrt{\sum_{i=1}^{n} y_i^2}}, \tag{3.4}$$

where

- $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ are two vectors in an n-dimensional space,
- $\text{CosineSimilarity}(x, y)$ measures the cosine of the angle between the two vectors, indicating their similarity, with values ranging from -1 (opposite directions) to 1 (identical directions).

$$\text{Accuracy} = \frac{1}{N} \sum_{i=1}^{N} I(\text{pos\_scores}_i < \text{neg\_scores}_i), \tag{3.5}$$

where

- N is the total number of samples,
- pos_scores_i represents the positive score for the i-th sample,
- neg_scores_i represents the negative score for the i-th sample,
- $I(\text{pos\_scores}_i < \text{neg\_scores}_i)$ is an indicator function that returns 1 if the condition $\text{pos\_scores}_i < \text{neg\_scores}_i$ is true, and 0 otherwise,
- $\sum_{i=1}^{N} I(\text{pos\_scores}_i < \text{neg\_scores}_i)$ counts the number of times the positive score is less than the negative score.

The choice of evaluation indicators is crucial to assess the effectiveness of SNN-based models in user authentication tasks. This thesis focuses on metrics focusing on indicators such as EER and accuracy, thus ensuring a balanced assessment of the model's ability to distinguish legitimate users from imposters. By highlighting EER as a key indicator, its importance in biometric authentication systems is highlighted in Table 1.1, as it is a comprehensive measure of the reliability of the system.

3.3. Experiments and Results Using CMU Dataset

The experiments in this section evaluate the proposed methodology for user authentication using the Carnegie Mellon University [56] dataset, which is a widely accepted benchmark in the field of keystroke dynamics research.

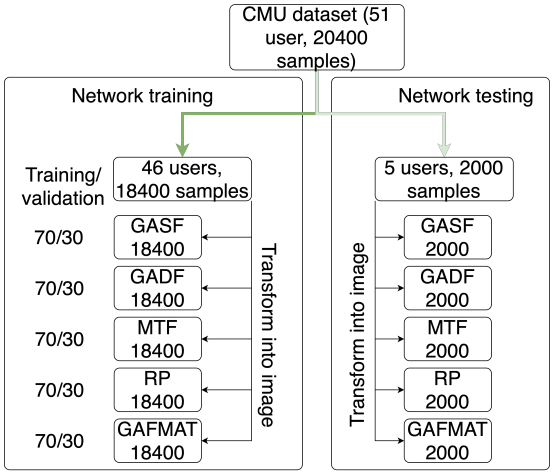


Figure 3.1: The process of preparing CMU data for model training/validation and testing

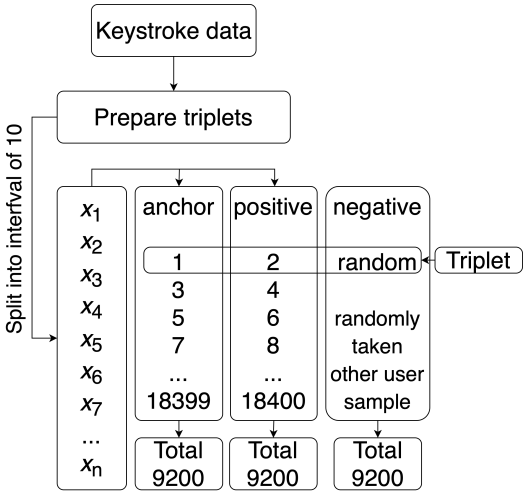


Figure 3.2: Splitting CMU data into the anchor and positive samples for each transformed dataset using the GASF, GADF, MTF, RP, and GAFMAT methods for triplet preparation

Before starting data analysis, a random selection was made to exclude the data of five users (see Figure 3.1), resulting in a data set comprising 46 individuals with 18,400 samples. The data excluded from those five users, consisting of 2,000 samples, were placed in a separate folder for testing purposes. This segregation was intended to ensure that the network would not be exposed to any of this data during the network training phase. Password samples from both the training/validation folder (18,400 samples) and the testing folder (five users with 2,000 samples) were transformed into image representations. This process yielded five datasets for network training/validation, each processed using different conversion methods (GASF, GADF, MTF, RP, GAFMAT). Additionally, five folders were created, each containing samples (images) of five users for network testing using the same transformation methods. In each dataset, each user entered the password 400 times, which were then split into two equal parts of 200 attempts each. The system alternated trials to classify the user's password entry behavior. Specifically, every second trial was considered an anchor sample of the user's password behavior, and the trials immediately following it were considered positive samples (see Figure 3.2). This division was based on the observation that users who become familiar with the password improve their typing speed over time and develop a more stable typing pattern. Therefore, when comparing anchor samples with positive samples, one should compare those which, over time and with the learning of the password, would not have drifted apart between trials. As a result, each dataset consisted of 9,200 positive samples (images) and 9,200 anchor samples (images). 70% of created triplets were used for training and the remaining 30% for validation. Additionally, for testing purposes, 1,000 positive images and 1,000 anchor images were extracted for the test datasets. To create training triplets for SNN, the anchor and positive samples were taken from the same user, while the negative sample was randomly selected from a different user. This procedure was repeated for each dataset with different conversion methods.

In the experiment, triplets were fed as input to SNN, and a margin size of 0.5 ($m = 0.5$, see (2.3)) was used. This decision was based on previous studies carried out to determine the optimal margin for different experimental configurations [B.1, B.2].

SNN was trained using the Adam optimizer over 100 epochs. To

prevent overfitting, an early stopping function was enabled, which stopped training if the model's performance on the validation dataset did not improve. In addition, a batch size of 128 was chosen for efficient computation and optimization. The batch size was determined after a series of experiments to find the balance between computational efficiency and model performance. The validation dataset was used to monitor the performance of the model, and the best weights were saved based on the validation loss. Following training, the optimal weights from each training epoch were saved, resulting in the storage of five sets of different network weights related to GADF, GASF, MTF, RP, and GAFMAT.

Table 3.2 summarizes the results obtained by each of the different transformation methods applied to the validation dataset. The results are evaluated according to the metrics described in Section 3.2. The data in the table indicate that the most accurate methods were GADF, with an accuracy of 0.99077, and GAFMAT, with an accuracy of 0.98935. Using RP and GASF, the values obtained were 0.98331 and 0.98473, respectively. In contrast, the MTF showed a noticeably lower accuracy of 0.94744.

Table 3.2: Results of image transformation methods on keystroke dynamics data from the CMU dataset using the GADF, GASF, RP, MTF, and GAFMAT algorithms: Metrics-based evaluation on validation data

	Non-Image to Image Transformation Methods				
Metrics	**GADF**	**GASF**	**RP**	**MTF**	**GAFMAT**
Accuracy↑	**0.99077**	0.98473	0.98331	0.94744	0.98935
EER↓	0.04794	0.05540	0.05327	0.12074	**0.04545**
AUC↑	0.98612	0.98290	0.98394	0.94862	**0.98668**
AP_ED↓	0.44127	0.47255	**0.43633**	0.56487	0.48600
AN_ED↑	1.72784	1.71689	1.68884	1.59469	**1.76378**
AP_STD↓	**0.27487**	0.29295	0.28245	0.36906	0.31383
AN_STD↓	0.32888	0.34455	0.34881	0.40005	**0.31295**
AN_CS↓	0.45772	0.45264	0.46871	0.46011	**0.43755**
AP_CS↑	0.77936	0.76373	**0.78183**	0.71756	0.75700

The results in Table 3.2 suggest that GADF outperforms the other methods in terms of AP_STD and accuracy, yielding slightly better results than the others. This implies that the positive images are positioned

closer to the anchor. However, the higher AN_ED values for GADF indicate that the method struggles to distinguish negative images from the anchor, in contrast to the superior performance of GAFMAT, which achieved an AN_ED value of 1.76378. A higher AN_ED value suggests that the other methods possess the ability to better discriminate negative images relative to the anchor. In summary, although GADF excels in proximity to the anchor with its lower AP_ED, and its comparative weakness in distinguishing negative images is evident from the higher AN_ED values. GADF exhibited the lowest AP_STD value of 0.27487, indicating less variability within the anchor and positive samples. Similarly, GADF had the highest AN_STD value of 0.32888, indicating more variability within the anchor and negative samples. This trend was also observed for the other methods. It should be acknowledged that explicit tests of statistical significance for these metrics were not performed in this thesis. Although there are notable differences in the results, for example, GAFMAT achieved a slightly better EER of 0.04545 compared to GADF 0.04794. It is unlikely that this small numerical improvement represents a statistically significant advantage. However, the author emphasizes that in a large number of repeated experiments with different batches, the GAFMAT method consistently showed the smallest range of variation in EER values, indicating greater stability and reliability of its performance.

The GADF has the highest AP_CS value of 0.77936, indicating a high cosine similarity between the anchor and positive samples. On the other hand, GADF also had the highest AN_CS value of 0.45772, indicating a relatively high cosine similarity between the anchor and negative samples. The other methods showed similar patterns, where GADF generally had higher AP_CS and AN_CS values. In the context of cosine similarity, a higher value is generally considered better. When the cosine similarity between two vectors (anchor and positive or anchor and negative) is closer to 1, the vectors point in a similar direction and have a higher degree of similarity. This is beneficial in many applications where similarity or correlation between vectors is important, and can be useful in a variety of tasks, such as document similarity, recommender systems, and pattern recognition.

From Table 3.2, it can be observed that the lowest EER value of 0.04545 was obtained using GAFMAT. This indicates a lower threshold

at which the trade-off between FAR and FRR is achieved. Other methods also showed relatively low EER values, except for the MTF, which had a higher EER of 0.12074. The highest AUC value (0.98668) was obtained using the GAFMAT method. The GADF method yielded results close to those of GAFMAT, with a value of 0.98612. The use of GASF and RP resulted in AUC values of 0.9829 and 0.98394, respectively. The MTF had a slightly lower AUC value of 0.94862.

In a comprehensive evaluation, the use of the GAFMAT and GADF methods showed promising results in several metrics, such as accuracy, distance measure, cosine similarity, EER and AUC. The empirical results highlight the potential effectiveness of GAFMAT and GADF as transformation methods for dataset analysis compared to the other methods considered.

In the following research, a comparative analysis was performed to evaluate the effectiveness of different transformation methods in a test dataset. The test dataset consists of previously unseen data samples that were processed using the same transformation method. By evaluating the results obtained from each method, the aim was to gain insights into their effectiveness and identify possible variations in performance (see Table 3.3).

Table 3.3: Results of image transformation methods on keystroke dynamics data from the CMU dataset using the GADF, GASF, RP, MTF, and GAFMAT algorithms: Metrics-based evaluation on test data

	Non-Image to Image Transformation Methods				
Metrics	**GADF**	**GASF**	**RP**	**MTF**	**GAFMAT**
Accuracy↑	**0.86800**	0.8540	0.82900	0.85400	0.86600
EER↓	**0.21000**	0.24500	0.23900	0.24500	0.21500
AUC↑	0.85928	0.83398	0.83937	0.83398	**0.85951**
AP_ED↓	**0.73164**	0.86555	0.84481	0.86555	0.83616
AN_ED↑	1.41323	1.50249	1.50904	1.50249	**1.52453**
AP_STD↓	**0.41727**	0.45697	0.47537	0.45697	0.44798
AN_STD↓	0.43871	0.44504	0.44953	0.44504	**0.42488**
AN_CS↓	0.46378	**0.40799**	0.41154	**0.40799**	0.40983
AP_CS↑	**0.63418**	0.56723	0.57760	0.56723	0.58192

The results of the validation data provided in Table 3.2 indicate clear variations in the performance of the different methods, with some

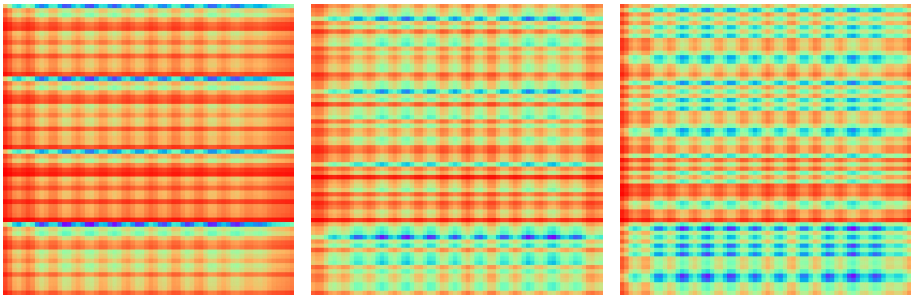
methods demonstrating better performance than others. However, it is important to highlight that the results obtained from the test data (see Table 3.3) are significantly lower than those obtained on the validation data. These differences are consistent across the test dataset, indicating that the performance differences observed in the validation dataset are also valid for the test data. The accuracy of the models decreased by approximately 10% to 0.86, and EER increased from 0.05 to approximately 0.20. This outcome suggests that SNN incorrectly classifies one out of every five negative samples as positive, highlighting a significant rate of false positives. However, the analysis shows the promise of using the GAFMAT and GADF methods over other methods in the analysis of the test data set.

3.4. Experiments and Results Using GREYC-NISLAB Dataset

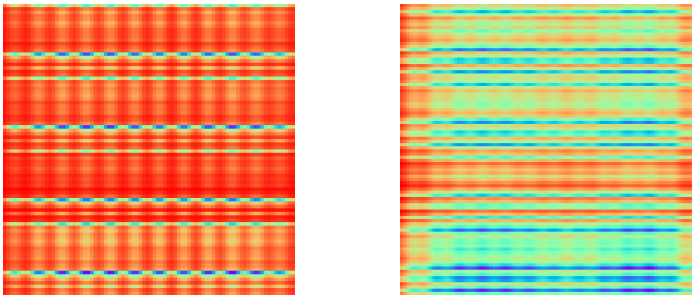
In the initial phase of the experiments using the CMU dataset, it was empirically determined that the proposed GAFMAT method achieved the lowest EER value. Therefore, to further validate the effectiveness of the proposed methodology, the analysis was extended to include an additional dataset of fixed-text passwords. These additional experiments allowed us to evaluate the effectiveness of the GAFMAT method on different datasets and to perform validation comparisons with results reported in related works.

The GREYC-NISLAB dataset described in Subsection 2.2.1 was collected in 2013 and includes five passwords entered by 110 users. The passwords are as follows: a) "leonardo dicaprio", b) "the rolling stones", c) "michael schumacher", d) "red hot chilli peppers", e) "united states of america" (note: the spelling is as provided in the original data file). Each user entered five different passwords ten times with both hands and ten times with one hand, depending on whether the user was left- or right-handed. The dataset of a single password consists of 2,200 samples. In total, the dataset comprises 11,000 data samples corresponding to 110 users, with 20 samples per user. Each password has different keystroke patterns, so the number of keystroke dynamics features ranges from 64 to 92. Using the GAFMAT method, each password was transformed into the corresponding graphical representations, resulting in password images (see Figure 3.3).

The experiments were carried out according to the procedures de-



(a) leonardo dicaprio (b) the rolling stones (c) michael schumacher



(d) red hot chilli peppers (e) united states of america

Figure 3.3: Image-based representations of distinct passwords of the same user, generated using the GAFMAT algorithm. Password data source: GREYC-NISLAB dataset

scribed in Section 3.3. The last five users from each password set were selected for testing. The final 2,100 samples from each password dataset were split at a 70:30 ratio into training and validation sets. The results obtained from the validation data were very similar to those from the CMU dataset and are presented in Table 3.4. The results were evaluated according to the metrics described in Section 3.2.

As shown in Table 3.4, the network could classify each password with an average accuracy of 0.98. Notably, the highest accuracy was achieved for the passwords "united states of america" and "michael schumacher", both with a high accuracy of 0.99. Using the Euclidean distances between the anchor and the positive sample (AP_ED), as well as between the anchor and the negative sample (AN_ED), the network was able to effectively detect differences between the positive and negative samples with respect to the anchor. As a result, the triplet loss function resulted in a decrease in the distance between the anchor

Table 3.4: Results using different accuracy metrics for passwords from GREYC-NISLAB on a validation dataset when transforming time series features of keystroke dynamics into an image using the GAFMAT algorithm

Metrics	Passwords (GREYC-NISLAB)				
	leonardo dicaprio	**the rolling stones**	**michael schumacher**	**red hot chilli peppers**	**united states of america**
Accuracy↑	0.97656	0.98698	0.99219	0.97778	**0.99220**
EER↓	0.07552	0.04688	0.06510	**0.04444**	0.04688
AUC↑	0.97824	0.98667	0.98771	0.98272	**0.98847**
AP_ED↓	0.44736	0.43986	0.39958	0.45165	**0.39566**
AN_ED↑	1.55644	1.61202	1.48864	**1.63478**	1.61275
AP_STD↓	0.24318	0.21992	0.20467	0.21505	**0.19676**
AN_STD↓	0.40601	**0.37381**	0.38351	0.38917	0.38013
AN_CS↓	0.49905	0.48703	0.52795	**0.47839**	0.49790
AP_CS↑	0.77632	0.78007	0.80021	0.77417	**0.80217**

and the positive samples to a range of 0.39 to 0.45 and an increase in the distance between the anchor and the negative samples to a range of 1.48 to 1.63. These metrics highlight the crucial difference between positive and negative samples in metric space. These empirical results underscore the effectiveness of the choice of a 0.5 margin based on the experimental results presented in [B.1, B.2].

The standard deviation of the distance between the anchor and the positive samples is approximately 0.2, and that between the anchor and the negative samples is approximately 0.39. This indicates that the network tended to admit more positive samples than negative samples, as the positive samples were twice as dispersed compared to the mean.

Another metric for quality evaluation, cosine similarity, was effective in distinguishing between positive and negative samples in relation to the anchor. The cosine similarity indicates that the positive sample is oriented in one direction relative to the anchor, with a value of approximately 0.78. In contrast, the negative samples are oriented in the opposite direction and have a value close to 0.5 relative to the anchor sample.

The most important indicator for validating the proposed GAFMAT

Table 3.5: Results using different accuracy metrics for passwords from GREYC-NISLAB on a test dataset when transforming time series features of keystroke dynamics into an image using the GAFMAT algorithm

Metrics	Passwords (GREYC-NISLAB)				
	leonardo dicaprio	**the rolling stones**	**michael schumacher**	**red hot chilli peppers**	**united states of america**
Accuracy↑	0.84000	0.86000	0.86000	0.84000	**0.92000**
EER↓	0.16000	0.20000	0.22000	0.22000	**0.14000**
AUC↑	**0.90320**	0.85920	0.85400	0.86680	0.89240
AP_ED↓	0.78894	0.86642	**0.67407**	0.87670	0.75085
AN_ED↑	**1.55808**	1.49985	1.33055	1.55131	1.50073
AP_STD↓	0.41371	0.40861	**0.31141**	0.44201	0.43587
AN_STD↓	**0.40956**	0.41111	0.49554	0.40963	0.42794
AN_CS↓	0.41324	0.40843	0.49884	**0.39300**	0.43711
AP_CS↑	0.60553	0.56679	**0.66297**	0.56165	0.62458

method is EER. For three specific passwords ("the rolling stones", "red hot chilli peppers", "united states of america"), the EER value varied by approximately 0.045. Moreover, for the "leonardo dicaprio" and "michael schumacher" passwords, the EER values are 0.07552 and 0.0651, respectively. Obviously, for the three passwords, the proposed methodology and approach provided an almost similar EER to the CMU dataset. However, it is important to note that the sample sizes of the datasets are different. The CMU dataset contains 400 instances of the same password for each user, while the GREYC-NISLAB dataset contains only 20 samples for each user.

After obtaining the validation results, an experiment was conducted on the test dataset to determine whether the password length would yield better results on unseen data. Before the training phase, a subset of five users was selected from each password dataset, allowing 100 samples to be analyzed for each individual password. After the training process, during which the optimal weights values were stored, the network was initialized with these parameters. The results of the evaluation using the unseen test data corresponding to the five users mentioned above are summarized in Table 3.5. The analysis shows that the results for the test data have a similar tendency to those for the

validation data, although their values have decreased. As shown in Table 3.5, the accuracy decreased to approximately 0.85. The Euclidean distances between the anchor and the positive samples increased, ranging from 0.67 to 0.87. In contrast, the distances between the anchor and negative samples remained almost the same as those in the validation data (see Table 3.4). Such observations suggest that even when assessing the quality using test data, the network retains the ability to distinguish between positive and negative samples compared to the anchor. This trend is also observed for the standard deviation. Although AN_STD remains the same as that for the validation dataset, remaining in the range of 0.4 to 0.49, AP_STD decreases by almost half compared to the Euclidean anchor-positive distance (AP_ED).

Since the objective in this case is to minimize EER, this indicator is treated as a baseline, which in the analysis of the GREYC-NISLAB dataset ranges between 0.14 and 0.22 for the test data, as shown in Table 3.5. The user authentication paradigm of the network is formulated in such a way that it can compare a newly entered password, transformed according to the GAFMAT technique, with previous entries, aiming to achieve an EER close to zero. Currently, an EER of approximately 0.2 is observed, which indicates that improvements are necessary. To summarize, the SNN with a triplet loss function is able to distinguish between positive and negative samples in the test data. However, the accuracy values obtained are definitely lower than those of the validation data.

3.5. Overview of Results from CMU and GREYC-NISLAB Datasets

The observed EER values indicate that the accuracy of this metric is affected by the length of the password. This is supported by the fact that the CMU dataset contains 31 features and the GREYC-NISLAB dataset contains 64 to 92 password features. In particular, EER for the password "united states of america", which is the longest in the set with 92 features, was 0.14 (see Table 3.5). EER of the next longest password, "red hot chilli peppers", with 84 characteristics, was 0.22. These observations suggest that EER is influenced mostly by the password's inherent features rather than its length.

The empirical findings from the experiments conducted on the CMU

and GREYC-NISLAB datasets were used to assess the performance of the newly proposed GAFMAT algorithm. The EER results of the validation phase of the CMU dataset were compared with the results of previous studies and showed a better performance of the GAFMAT method (see Table 3.6). This analysis highlights the effectiveness of GAFMAT in improving biometric authentication through improved accuracy and feature mapping. It should be noted that many published papers report results based mainly on validation data. Therefore, comparative analysis with other studies is performed using EER results on the validation data from the CMU dataset. EER results on the test data of the GREYC-NISLAB dataset are used for comparative analysis with a recent study on user authentication [82].

Table 3.6: Performance evaluation for CMU dataset passwords on validation data: a comparison of results in terms of EER values

References	**Method**	**EER**
Section 3.3	GAFMAT	**0.04545**
[56] (original)	Manhattan distance (scaled)	0.09600
[116]	Nearest neighbor (new distance metric) + outlier removal	0.08400
[116]	Nearest neighbor (new distance metric)	0.08700
[73]	Inductive transfer encoder (Manhattan distance)	0.06300
[18]	CNN	0.06500
[49]	Dependence clustering with Manhattan distance	0.07700
[87]	Manhattan distance (scaled with standard deviation)	0.09160

Table 3.6 presents a focused performance evaluation of EER of different methods using the CMU dataset. It aims to emphasize advances in EER reduction on CMU data. The method based on the Manhattan distance (scaled) reported by [56] showed EER of 0.096, indicating less efficiency in balancing false acceptances and false rejections. In contrast, the nearest-neighbor method with a new distance metric, as explored by [116], showed EER of 0.084 with outlier removal and 0.087 without it. Similarly, the inductive transfer encoder approach, applied by [73],

resulted in an EER of 0.063, which, although closer to the result of the GAFMAT method, remains less optimal. CNN used by [18] achieved an EER of 0.065, indicating fairly good performance. In addition, methods such as dependency clustering with Manhattan distance [49] and Manhattan distance (with standard deviation scaling) [87] showed EERs of 0.077 and 0.0916, respectively, indicating lower and insufficient authentication accuracy. This comparative analysis clearly indicates that the GAFMAT method significantly outperforms existing methods in terms of authentication accuracy, as evidenced by its significantly lower EER in the context of the CMU dataset. The results highlight the potential of the GAFMAT method for more accurate and reliable user authentication in cybersecurity applications. The performance of the proposed method was specifically compared to that of studies that used the complete sample set of the CMU dataset without excluding outliers, in contrast to a previous study [73] in which outliers were removed, resulting in EER of 0.047, but an overall EER of 0.063. In the paper [87], the highest EER of 0.045 was obtained, but these results are only for "good" users. The authors of the paper set the FAR threshold and calculated what EER would be for "good", "average", and "bad" users. Despite these results, the average EER of 0.0916 of all users was taken and compared with the results obtained by the methods presented in this paper [87].

The results obtained on the CMU dataset indicate that transforming the numerical values into images using techniques such as GADF, GASF, and RP resulted in EER values of 0.04794, 0.0554, and 0.05327, respectively (see Table 3.4). These findings highlight the effectiveness of the proposed approach for transforming passwords into images to train SNN, which improved the performance over previous state-of-the-art methods. Significantly, proposed method for converting numerical data into images, called GAFMAT, achieved an improved EER value of 0.04545 (see Table 3.6).

A comparative analysis of the validation and test results of the GREYC-NISLAB dataset was carried out, with particular regard to the evaluation of their performance in terms of EER and accuracy. This choice was made because recent research on this user authentication task dataset has focused on improving accuracy and achieving better EER values [82]. This thesis, therefore, aimed to compare the results with these established benchmarks.

The information in Table 3.5 allows comparison of this thesis results with those of other authors [82]. As indicated in this study, the best results for EER using the GoogleNet model were 0.1843 for "leonardo dicaprio", 0.1423 for "michael schumacher", and 0.148 for "united states of america". Meanwhile, this thesis proposed methodology with the implemented GAFMAT method achieved EER values of 0.16, 0.22, and 0.14, respectively. Notably, the implementation of a 12-layer CNN, while not as deep as the 22-layer deep neural network (GoogleNet), yielded results on the test dataset that are comparable to or slightly better than the network containing almost twice as many layers.

The results obtained on CMU data clearly demonstrate that the proposed GAFMAT method combined with SNN achieves slightly lower EER than do existing methods such as GADF, GASF, MTF and RP. The GAFMAT method also demonstrated a high stability across all experiments, producing reliable results regardless of changes in the data set or experimental conditions. The method achieved EER of 0.04545 on the CMU dataset. In addition, the method achieved a high level of accuracy for the GREYC-NISLAB dataset, with EERs ranging from 0.04444 to 0.07552. The findings emphasize the remarkable performance of the proposed solution in distinguishing genuine users from impostors.

3.6. Keystroke Dynamics Data Visualization Experiments and Results

Data visualization is essential in data analysis because it helps transform complex, high-volume information into an intuitive and understandable form. This process helps uncover patterns, trends, and anomalies that may remain hidden in raw data, facilitating more informative and effective decision making. Visualizing keystroke dynamics data is important for enhancing user authentication systems and detecting potential insider threats in critical infrastructure. This section presents a visualization framework that combines SNNs with dimensionality reduction techniques to analyze and interpret complex keystroke patterns.

In this thesis, the visualization process comprises several stages (see Figure 3.4), each with a specific purpose, to ensure that the data are accurately represented in a lower-dimensional space, facilitating analysis and decision-making. An expanded and detailed description of the process follows:

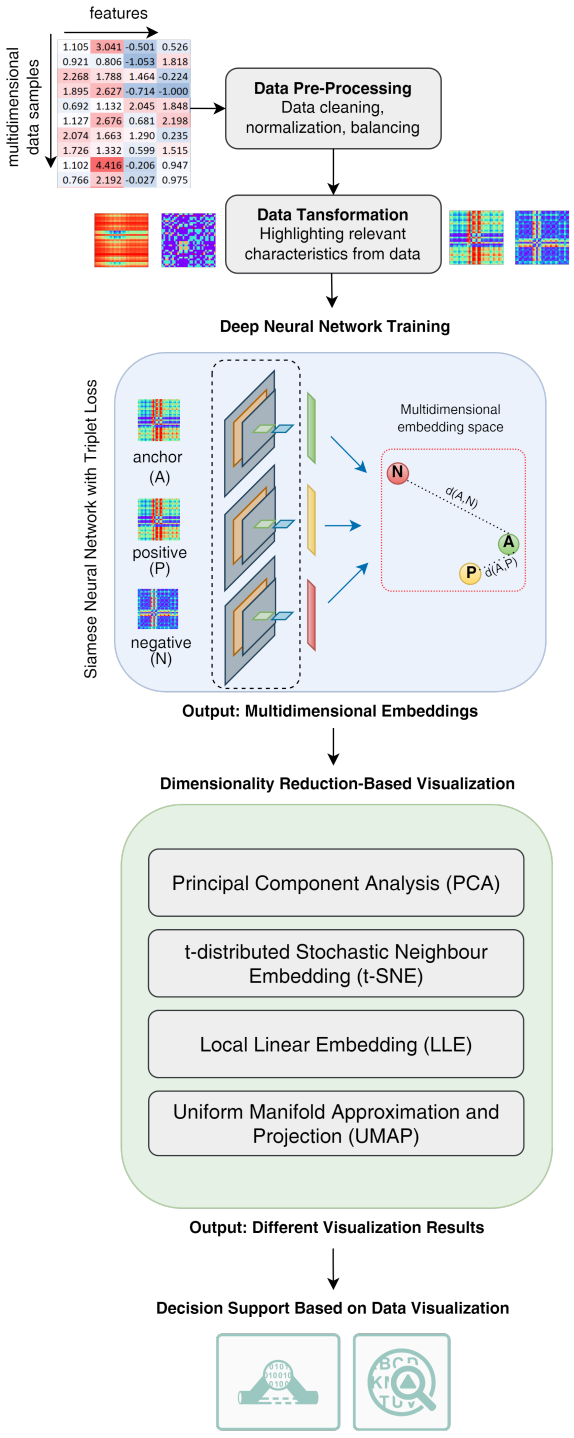


Figure 3.4: The visualization framework based on dimensionality reduction for multidimensional embedding analysis in decision support

- Data pre-processing. The raw keystroke time data from the analysed datasets (e.g. CMU) are cleaned, normalized, and balanced to prepare the raw data for subsequent steps.

- GAFMAT transformation. The preprocessed keystroke data are transformed into image representations using GAFMAT, as detailed in Subsection 2.2.3. This transformation enhances the ability of CNNs to extract relevant features from typing patterns.

- SNN training. The transformed keystroke images are processed through an SNN with CNNs branches, using the triplet loss function. This network learns to generate embeddings that effectively distinguish between legitimate users and potential impostors based on their typing patterns. These embeddings represent the similarities and dissimilarities between the data samples. In this way, each data sample is converted to a point in the embedding space.

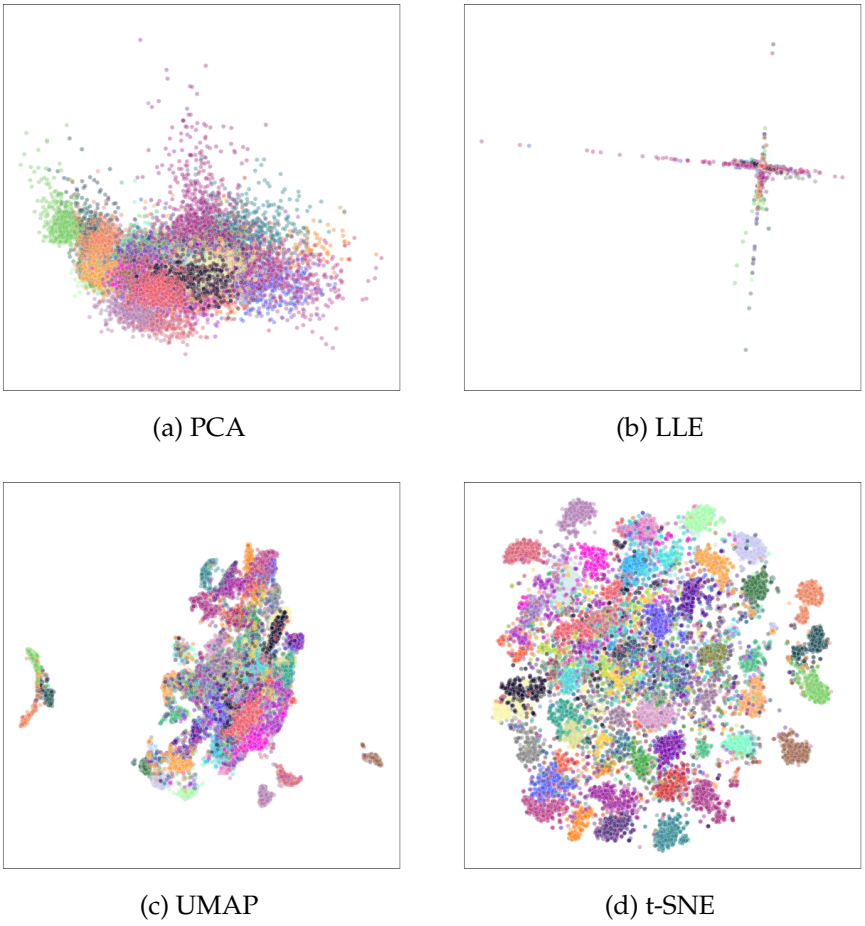
- Dimensionality reduction. The high-dimensional embeddings produced by SNN are projected into a two-dimensional space using techniques such as PCA, t-SNE, LLE, and UMAP. Each technique offers a different perspective on the keystroke data structure, potentially revealing unique insights into user typing behaviors.

- Authentication decision support. The resulting visualizations enable the identification of patterns, anomalies, and potential insider threats in keystroke dynamics. This visual analysis supports more informed decision-making in user authentication for critical infrastructure protection.

This visualization framework addresses several key aspects of the thesis. It demonstrates how SNNs with CNNs branches can learn discriminative features from keystroke dynamics transformed to the visual representations to authenticate users. A mean to visually detect potential insider threats by identifying anomalous typing patterns is proposed. By integrating deep learning with visualization techniques, this framework enhances the interpretability of complex keystroke dynamics data.

3.6.1. Use Case Analysis of Keystroke Dynamics for User Authentication

This subsection demonstrates the effectiveness of the proposed visualization framework for analyzing keystroke dynamics in user authentication. The experiments utilize the CMU dataset, which contains multidimensional data representing keystroke patterns from different users.



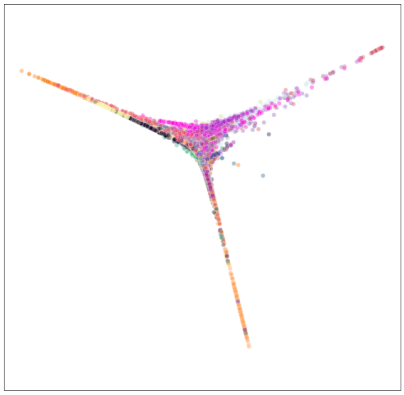
(a) PCA (b) LLE

(c) UMAP (d) t-SNE

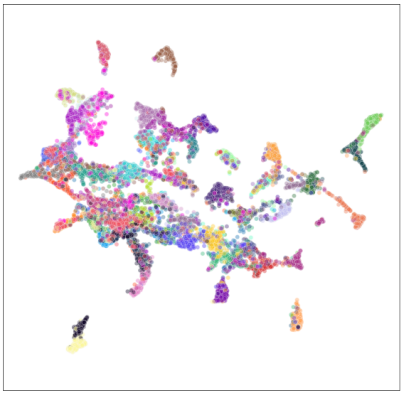
Figure 3.5: Multidimensional data visualizations using different dimensionality reduction techniques: (a) PCA, (b) LLE, (c) UMAP, (d) t-SNE. Each color corresponds to a different user in the CMU dataset

Figure 3.5 shows the results of applying various dimensionality reduction techniques (PCA, LLE, UMAP, and t-SNE) to the raw CMU dataset. These visualizations reveal that conventional methods struggle

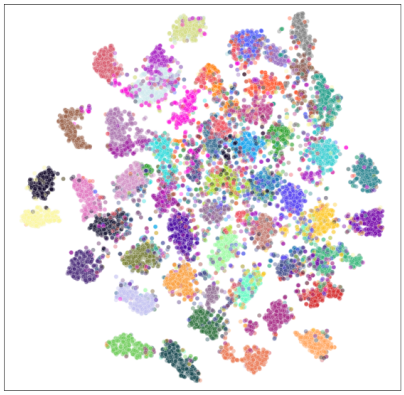
(a) PCA



(b) LLE



(c) UMAP



(d) t-SNE

Figure 3.6: Visualization of multidimensional embeddings obtained by SNN using different dimensionality reduction techniques ($p = 256$): (a) PCA, (b) LLE, (c) UMAP, (d) t-SNE. Each color corresponds to a different user in the CMU dataset

to clearly separate users based on their typing patterns, highlighting the need for more advanced approaches. Labels and units for both axes are omitted when presenting the visualization results in this and the following figures. This approach is driven by the focus on observing the inter-locations of points in 2D space. The proposed framework uses SNN with CNNs branches to generate multidimensional embeddings from the GAFMAT-transformed keystroke data. As a result of processing the raw data on keystroke dynamics transformed into images using SNN with triplet loss function, multidimensional embeddings are extracted. These

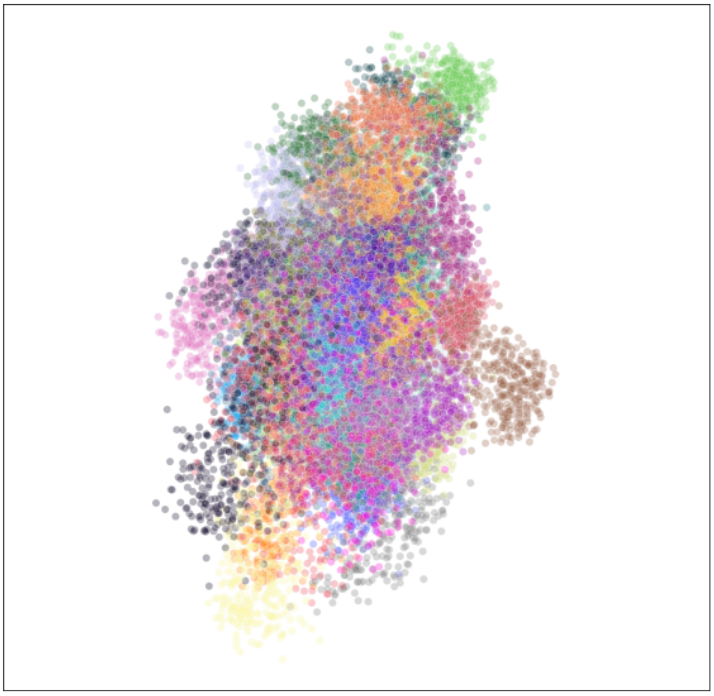


Figure 3.7: Visualization of two-dimensional embeddings ($p = 2$) obtained by Siamese neural network

embeddings, denoted as $E_i = (e_{i1}, \ldots, e_{ip})$, $i = 1, \ldots, m$, represent the keystroke patterns of each user in p-dimensional space, where $p \geqslant 2$. Each embedding E_i includes distinctive characteristics of keystroke dynamics, embedding the typing behavior in the p-dimensional feature space. Figure 3.6 presents the visualizations of these embeddings using the same dimensionality reduction techniques. Each color corresponds to a different user in the CMU dataset and represents individual behavioral profiles. The results show significantly improved separation between users, especially when using t-SNE. PCA shows a wide spread of points, but does not provide a clear view of the discrete clusters. LLE reveals some structure, but with a high degree of distortion. In the case of UMAP, it is possible to observe certain clusters, but the distinction between them is not sufficiently clear and obvious, which complicates the decision-making and does not allow for making appropriate and reliable decisions. In contrast, t-SNE allows for a clear distinction between clusters and specifies the unique typing patterns of different users.

The results obtained with the proposed framework (see Figure 3.4) and depicted in Figure 3.6 demonstrate the visualization results for embeddings with an initial dimensionality of 256. In order to test the hypothesis that the generation of multidimensional embeddings makes sense when their dimensionality is significantly higher than two ($p \gg 2$), it was decided to visualize the two-dimensional embeddings without applying any dimensionality reduction technique and to compare the resulting visualizations. The number of dimensions represents the number of outputs of SNN. The results can be seen in Figure 3.7. Here, the points corresponding to the users are scattered widely, and there are no distinct clusters. A comparison of Figures 3.6 and 3.7 justifies that embedding the data in a higher dimensional space using Siamese networks and visualizing the embeddings by dimensionality reduction techniques is meaningful.

To illustrate the performance of the proposed framework (see Section 3.4) it is meaningful to compare the visualization results of the raw multidimensional data (see Figure 3.5) and the multidimensional embeddings obtained by SNN (see Figure 3.6). The comparison results illustrate that multidimensional embedding visualization is more suitable for decision-making, as clusters corresponding to user's keystroke dynamics patterns are better separated and more clearly visible (see Figure 3.6). As demonstrated previously, the use of the t-SNE technique better reveals the structure of the patterns analyzed. Figure 3.5 (d) represents the visualization of the raw keystroke dynamics data using t-SNE. The clusters appear to be slightly more diffused, with some overlapping between different colors, indicating that while distinct user patterns can be observed, the separation is not as clear-cut. This poses a challenge for decision-making in user authentication, as the decision boundary between different users is not clear. As a result, a decision support system may have a higher rate of misclassification, leading to potential security vulnerabilities. Figure 3.6 (d) shows the visualization of multidimensional embeddings extracted by SNN using t-SNE. The clusters in this visualization are generally more distinct and separated from each other, with less overlap between colors. This suggests that the embeddings from SNN provide a more refined and discriminative representation of keystroke dynamics and improve the separation between different users. Such visualization results contribute to more confident authentication

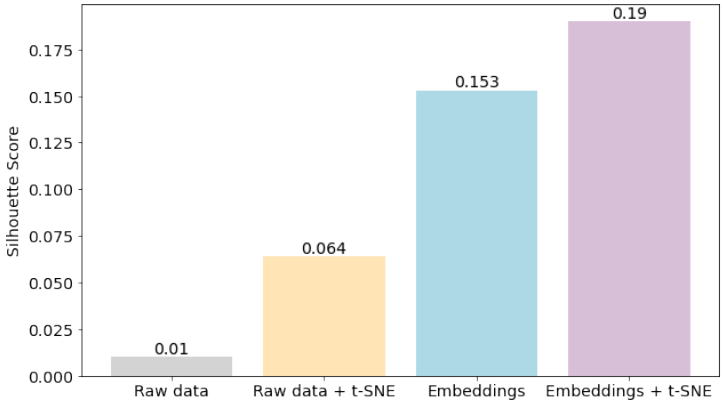
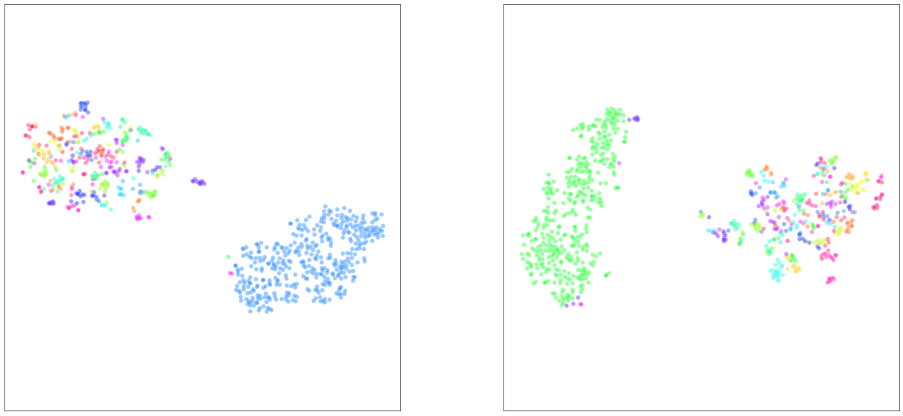


Figure 3.8: Silhouette scores before and after applying t-SNE on raw multidimensional data and their embeddings

decisions.

Furthermore, it is important to quantitatively evaluate how well the data in the lower-dimensional space represent the original data structure and relationships. After dimensionality reduction, the data points are often clustered. Figure 3.8 presents silhouette scores [94] for different stages of the visualization process, quantitatively demonstrating the improvement in cluster separation achieved by the proposed framework. The silhouette score helps determine how cohesive the clusters are internally and externally separated the clusters are.

As seen in Figure 3.8, the lowest silhouette score of 0.01 is obtained for the raw multidimensional data. It suggests that raw data do not naturally form well-defined clusters. This could be due to high dimensionality or inherent noise and variability in the data. Applying t-SNE to the raw data results in a higher silhouette score of 0.064. This improvement indicates that t-SNE helps in revealing some underlying structure of the data, making the clusters more distinct than in the raw data. When the raw data are transformed into images and the resulting images are used to train a SNN, the silhouette score for the multidimensional embeddings obtained at the network outputs is 0.153, which is a significant improvement over the raw data. This suggests that the embedding process effectively captures the essential features, leading to better clustering. The highest silhouette score is observed when t-SNE is applied to the multidimensional embeddings, reaching 0.190. This



(a) (b)

Figure 3.9: Examples of visualizations that show password typing patterns of the same user and the other randomly selected users

indicates that the combination of embedding techniques with t-SNE results in the most distinct and well-separated clusters of all analyzed data.

Figure 3.9 presents two examples of distinguishing a single user's typing patterns from those of other users. The application of this visualization process is demonstrated with two different examples, each representing a different user from the CMU dataset. Each case presents all samples of one user's keystroke data and compares them to 400 randomly selected samples of other users. These visualizations demonstrate the framework's ability to clearly separate legitimate users from potential impostors, which is crucial for enhancing authentication accuracy in critical infrastructure systems. However, in some cases, the writing behavior of other users is very similar to a legitimate user's, but still outside that user's cluster. This suggests that writing behavior may be replicated in some cases, underlining the importance of robust models to handle such a delicate correspondence. In Figure 3.9, the clusters of blue points represent the multiple password attempts of the selected user, while the multicolored points represent the randomly selected attempts of other users. This separation shows the similar password behavior of the selected user, whose pattern is clearly different from the other users. The same visualization approach is applied to the second example (the green cluster). In Figure 3.9, the user's data samples also form a

separate cluster that is distinguishable from the other user's samples. The consistency of the results in both examples confirms the validity of the multidimensional data visualization process. The silhouette scores of 0.690 (Figure 3.9, a) and 0.645 (Figure 3.9, b) justify the effectiveness of the visualization framework to distinguish between legitimate and illegitimate users based on their typing patterns using the CMU keystroke dynamics dataset.

This visualization framework complements the GAFMAT transformation and SNN-based authentication method described in previous sections by providing visual mean to analyze and validate the effectiveness of the proposed approach. It offers valuable insights for security analysts to detect anomalies and potential insider threats in critical infrastructure environments. The visualization process is of particular importance in the context of cybersecurity applications, as it allows SOC analysts to monitor and analyze triggered anomalies visually, thus enhancing their ability to detect and respond to potential threats in critical infrastructure. The ability to distinguish between user behavior patterns through visual means has the potential to markedly enhance decision-making processes in both anomaly detection and user authentication systems.

3.7. Keystroke Dynamics Data Fusion-Based Experiments and Results

Keystroke dynamics standardization is the key for developing deep learning-based models that can accommodate passwords of varying lengths, thereby creating a more accurate and universal user authentication system. This section details a series of experiments aimed at demonstrating the effectiveness of the proposed data fusion approach (Section 2.5) in handling keystroke dynamics data from different lengths, emphasizing its capability to enhance user authentication. In a series of experiments, the aim was to demonstrate the effectiveness of the data fusion approach when dealing with passwords of different lengths and, consequently, with different numbers of timestamps. These experiments were designed not only to validate the feasibility of proposed method, but also to identify the most effective strategies for fusing keystroke dynamics datasets. In this way, the thesis aims to demonstrate the enhanced capabilities of the proposed approach in distinguishing gen-

uine user actions from potential security threats or insiders, thereby improving the quality of user authentication processes.

CNN architecture used for SNN, which was designed to process 37x37 input images, is presented in Table 3.7. Each convolutional layer is followed by batch normalization, dropout, and max pooling operations. This sequence is followed by a flattened layer, whose output is used as input to the dense layer. The final dense layer has 256 outputs. The network output can be considered as an embedding of the original input. Each layer utilizes the Rectified Linear Unit (ReLU) activation function to introduce nonlinearity, which enhances the learning ability of the network. The network, which has a depth of 13 layers, covers a total of 2,806,496 parameters.

When separating the dataset for training, validation, and testing a neural network, the goal is to estimate the model's performance as realistically as possible. However, separating data from the same user into training and validation sets can introduce bias and result in overly optimistic performance measures. This is because the model may simply recognize a particular user rather than generalizing the obtained performance. To ensure that the generalization capabilities of the model are accurately estimated, it is important to have different users in the training, validation, and test sets. This separation ensures that the evaluation is based on the model's ability to learn and apply patterns to new, unseen data, which is a more accurate measure of its effectiveness in the real world. In this thesis, experiments adopted a 70/15/15 split for training, validation, and testing, respectively. A subset of users from each dataset (15%) was used for validation to observe the performance of the network during training. The other 15% of users were allocated for testing and stored separately to evaluate the network's performance on previously unseen data. This separation of data allows us to better simulate real-world conditions when the model encounters data that it did not encounter during training.

3.7.1. Keystroke Dynamics Data Fusion Result Validation

In this thesis, ANOVA [38] was used to assess the statistical significance of the differences in the means of EERs obtained by the different interpolation methods. This method allows us to determine whether the differences in EER means obtained are statistically significant or whether

Table 3.7: Summary of the convolutional neural network architecture used in the Siamese neural network for keystroke dynamics authentication

Layers	Output Shape	Number of Parameters
InputLayer	(None, 37, 37, 3)	0
Conv2D	(None, 37, 37, 32)	1,568
BatchNormalization	(None, 37, 37, 32)	128
Dropout	(None, 37, 37, 32)	0
MaxPooling2D	(None, 18, 18, 32)	0
Conv2D	(None, 18, 18, 64)	18,496
BatchNormalization	(None, 18, 18, 64)	256
Dropout	(None, 18, 18, 64)	0
MaxPooling2D	(None, 9, 9, 64)	0
Flatten	(None, 5,184)	0
Dense	(None, 512)	2,654,720
Dropout	(None, 512)	0
Dense	(None, 256)	131,328

they can be explained by chance. The analysis of the differences between the mean EERs obtained by the cubic, linear, and nearest-neighbor interpolation methods for the CMU dataset showed a p-value of 0.2916 for the time series data interpolation. Additionally, EERs for image post-resizing using interpolation techniques such as bicubic, bilinear, and nearest-neighbor methods, which yielded a p-value of 0.1472. Examining the variance of the mean EERs of the KeyRecs dataset obtained by the cubic, linear, and nearest neighbor interpolation methods, it was found that the p-value was 0.1016 for the time series interpolation and 0.0889 for post-resizing with interpolation. These results (see Table 3.8), above the usual alpha level of 0.05, indicate that there are no statistically significant differences in the efficiency of the interpolation methods at the significance level 5%. This finding suggests that the observed differences in EER between the interpolation methods can be explained by random variation rather than by a definite difference in performance.

Boxplots are commonly used to visually compare the performance of interpolation methods for different data sets. This section presents the performance measures for the test datasets. Figures 3.10 and 3.11 show EERs for different interpolation methods (linear, cubic, nearest

Table 3.8: Statistical significance (p-values) of different interpolation methods and post-resizing image interpolation methods applied to the CMU and KeyRecs datasets. A p-value derived from ANOVA tests greater than 0.05 indicates no statistically significant difference between the methods

Dataset	**Interpolation Methods**	p**-value**
CMU	Time series interpolation (Linear, Cubic, Nearest Neighbor)	0.2916
	Post-resizing with interpolation (Bicubic, Bilinear, Nearest Neighbor)	0.1472
KeyRecs	Time series interpolation (Linear, Cubic, Nearest Neighbor)	0.1016
	Post-resizing with interpolation (Bicubic, Bilinear, Nearest Neighbor)	0.0889

neighbor) applied to time series and for image post-resizing with interpolation (bilinear, bicubic, nearest neighbor) using the CMU and KeyRecs datasets, respectively. Boxplots are often used because they summarize the distribution of data points in a concise way, showing the median, mean, quartiles, and outliers, thus illustrating the tendency and variability of the data. In the boxplot, the center line indicates the median EER for each method. The boundary extends from the first to the third quartile, showing the middle of the data range. The whiskers extend to the farthest points that are not considered outliers. Outliers are shown as individual points outside the whiskers. The triangle indicates the mean EER for each method.

Figure 3.10 shows a comparison of how different interpolation methods affect EER for both time series and post-resizing images. Boxplots for the CMU dataset show the distributions of EERs for all interpolation methods. Linear interpolation proves to be the most effective method on the CMU dataset, with a mean EER of 0.16462, indicating the high accuracy of this method. On the other hand, the nearest neighbor interpolation method on the post-resizing shows a slightly higher mean EER of 0.17187, and the corresponding cubic interpolation is approximately 0.17634. In particular, linear interpolation maintains not only the lowest mean EER but also the most concentrated interquartile range, indicating a high level of stability of the dataset. In contrast, the cubic and nearest-

neighbor methods show a larger variation in EER values, indicating less stability in performance. The implications of these findings are also emphasized by the bilinear post-resizing method, which demonstrates a mean EER comparable to that of linear interpolation but with marginally more variation. The smaller range of resizing with the bilinear interpolation method compared to resizing with the bicubic interpolation method suggests that it may be an intermediate option in terms of stability and accuracy. Table 3.9 supplements these observations by detailing the best, mean, and standard deviation (std) values for accuracy and EER, which provides a more complete understanding of the performance of each method. Lower EER values correlate with higher performance; thus, the low variability of the linear interpolation method confirms its suitability for the task at hand. Although nearest-neighbor interpolation competes with resizing using nearest-neighbor interpolation, its wider variability indicates its dependence on data specificity. In conclusion, linear interpolation is the most stable and potentially accurate method for the fusion of datasets, whereas bilinear interpolation can serve as an alternative if moderate variability is acceptable. The key point of the experiments was the best EER value achieved using linear interpolation, which was 0.13672. This value emphasizes the potential of linear interpolation not only for obtaining the most stable mean EER but also for achieving the lowest number of errors in specific cases.

Table 3.9: Performance metrics for the CMU dataset using different interpolation methods for time series standardization and image post-resizing

	Time series interpolation			Post-resizing with interpolation		
Metrics	Cubic	Nearest Neighbor	Linear	Bicubic	Nearest Neighbor	Bilinear
Accuracy (best)	0.94141	0.92969	0.91797	0.91406	0.94141	0.92578
Accuracy (mean)	0.91685	0.91574	0.90737	0.90234	0.91016	0.91016
Accuracy (std)	0.01282	0.01062	0.00828	0.00835	0.01235	0.01772
EER (best)	0.15625	0.15625	0.13672	0.15234	0.16016	0.16016
EER (mean)	0.17634	0.17913	0.16462	0.18025	0.17187	0.17188
EER (std)	0.01423	0.02007	0.01423	0.01376	0.01023	0.02738

After thoroughly evaluating the interpolation methods applied to the CMU dataset using both the original time series and post-resizing with interpolation, it was concluded that linear interpolation is the most appropriate approach for the efficient fusion of datasets. To further validate this conclusion, the thesis was extended to the KeyRecs dataset.

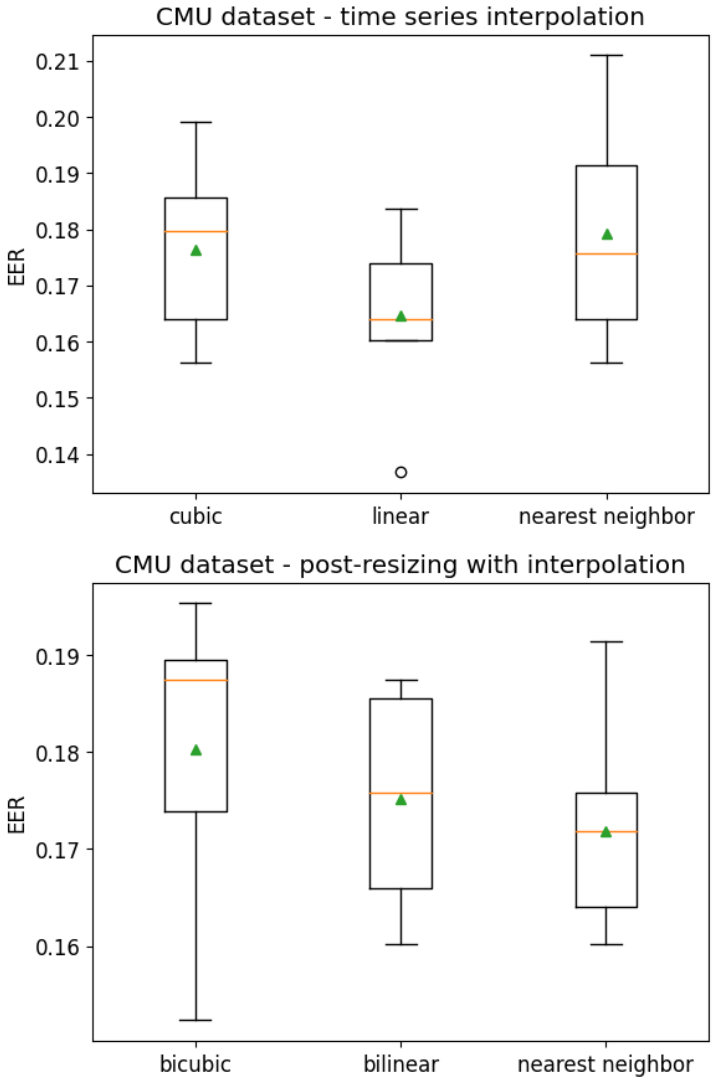


Figure 3.10: Comparison of equal error rates for the CMU dataset using different interpolation methods for data standardization: interpolation methods are used to standardize the length of the time series (top); images are post-resized using different interpolation methods (bottom)

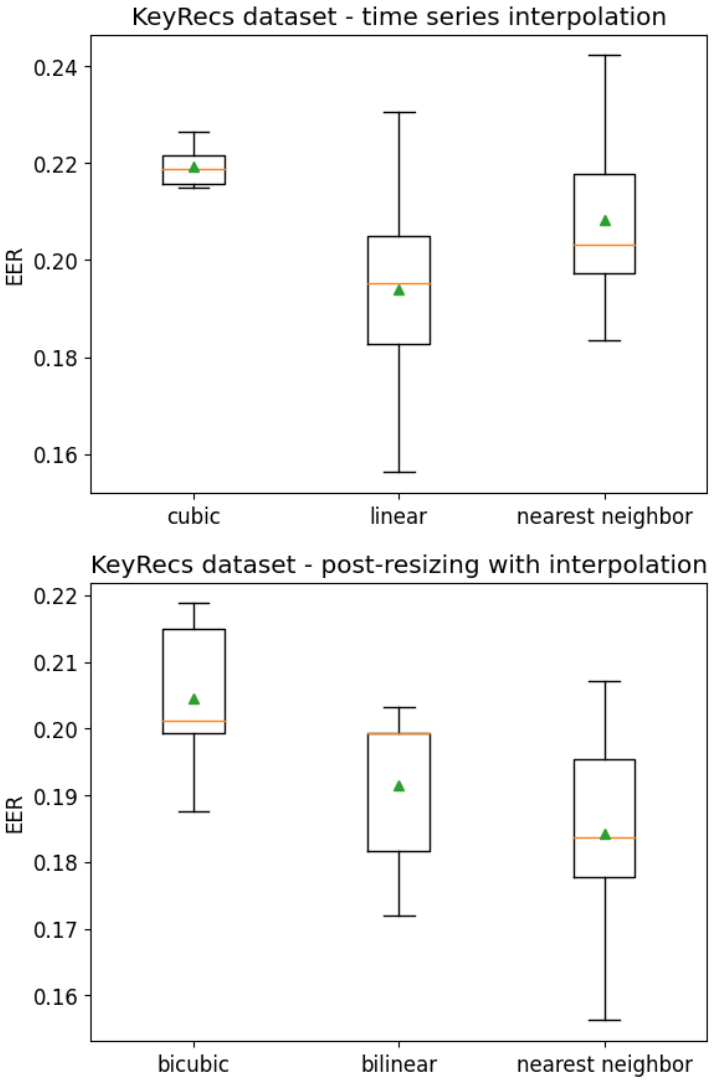


Figure 3.11: Comparison of EERs for the KeyRecs dataset using different interpolation methods for data standardization: interpolation methods are used to standardize the length of the time series (top); images are post-resized using different interpolation methods (bottom)

Table 3.10: Performance metrics for the KeyRecs dataset using different interpolation techniques for data fusion

Metrics	Time series interpolation			Post-resizing with interpolation		
	Cubic	Nearest Neighbor	Linear	Bicubic	Nearest Neighbor	Bilinear
Accuracy (best)	0.91406	0.90625	0.91406	0.89844	0.91016	0.90625
Accuracy (mean)	0.87956	0.89388	0.89779	0.88346	0.89388	0.89388
Accuracy (std)	0.01648	0.01264	0.01569	0.01159	0.01137	0.00941
EER (best)	0.21484	0.18359	0.15625	0.18750	0.15625	0.17188
EER (mean)	0.21940	0.20833	0.19401	0.20443	0.18424	0.19141
EER (std)	0.00417	0.01909	0.02296	0.01120	0.01633	0.01256

This set was chosen because of the similarity in password length to the CMU dataset but with a larger feature size. The results of applying different interpolation strategies to the KeyRecs dataset are shown in Figure 3.11, and the detailed results are presented in Table 3.10. Analyzing the post-resizing interpolation results using the KeyRecs dataset shows that the mean EER tends to be slightly lower than in the case of time series interpolation analysis. In particular, the mean EER for the bilinear and bicubic interpolation methods was slightly greater than 0.19, while the nearest neighbor interpolation method showed a mean EER value of 0.18424, although with significant variability. In time series interpolation, the linear interpolation method has consistently lower mean EER values, which is consistent with its performance on the CMU dataset. The bilinear image resizing method shows commendable results. Although its mean EER is slightly greater than that of its nearest-neighbor method, its more compact interquartile range indicates reduced variability, which provides more stable performance across different samples. The prominent result of this evaluation was the achievement of the best EER value of 0.15625 using linear interpolation on the KeyRecs dataset, which is an indication of the method's potential to provide strong user authentication on different datasets.

A comparative evaluation of the CMU and KeyRecs datasets revealed a definite relationship between the different interpolation strategies and the characteristics of each dataset, particularly in terms of accuracy and EER. This analysis shows that although the performance of the interpolation methods varies depending on the specifics of the dataset, linear interpolation consistently maintains high stability in all cases. This stable EER across different datasets emphasizes the effectiveness of linear interpolation and makes it the preferred data fusion

method for training neural network models. This is particularly relevant in scenarios requiring improved accuracy and reduced EER in different data contexts.

The analysis of the GREYC-NISLAB dataset presented in Figure 3.12 and Table 3.11 shows that the linear interpolation method applied to keystroke dynamics data with different initial feature lengths is quite promising. The GREYC-NISLAB dataset consisted of five different passwords, each corresponding to a significant person or phrase: "leonardo di caprio" (LDC), "michael shumacher" (MS), "red hot chilli pepper" (RHCP), "the rolling stones" (TRS) and "united states of america" (USA). This uniform feature transformation to 37 for a wide range of passwords demonstrates the potential of a generalized authentication solution capable of handling passwords of different lengths with significant efficiency. Notably, the obtained EERs for different passphrases indicate that the linear interpolation method performs well even after reducing the feature sizes, providing stable authentication performance. For example, the passwords associated with LDC and MS yielded mean EER values of 0.19792 and 0.18750, respectively, with relatively small standard deviations. This consistency indicates the ability of the method to retain the distinctive features of the set after feature compression, which is important for accurate user authentication. The highest variability of the password corresponding to the USA, which also had the longest initial feature length, raises the question of the scalability of the method when dealing with significantly long passwords. However, even in this case, the mean EER did not exceed 0.22396, which is relatively moderate and indicates some robustness of the method. Moreover, the better accuracy rates, especially for LDC and MS, confirm the potential of this approach. These performances indicate that even when the size of the feature is compressed, the important dynamics of individual keystrokes is largely preserved, which is promising for real-world applications where the password length can vary significantly. The most compelling aspect of this analysis is the best EER values achieved for the different passwords. In particular, the passwords associated with LDC, MS, RHCP, and USA achieved the best EER value of 0.15625, which is exceptionally low. This low EER is indicative of the high accuracy of the system, where false accepts and false rejects are minimized, thus providing a high degree of confidence in the authentication process. For TRS, the best EER is

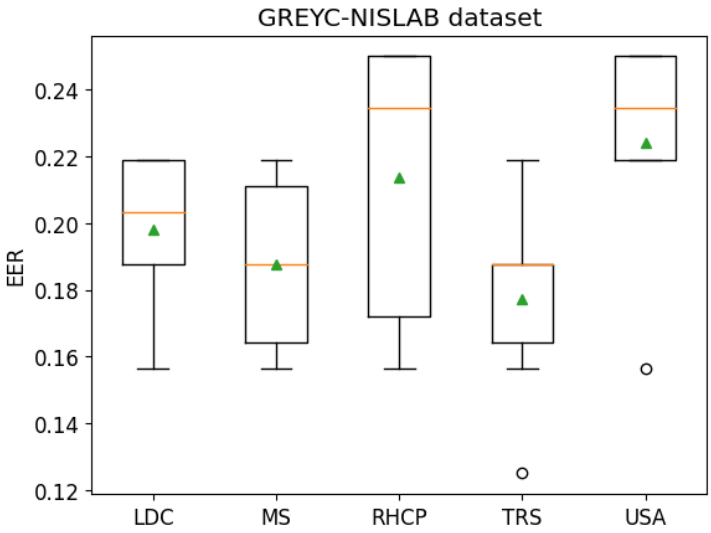


Figure 3.12: Comparison of EERs for all passwords in the GREYC-NISLAB dataset using linear interpolation, demonstrating the effectiveness of the proposed methodology when dealing with passwords of different lengths for user authentication

even lower at 0.1250, further emphasizing the potential of this approach. These best EERs are particularly important because they demonstrate the capabilities of the model. When considering such a system for critical infrastructure security, where accuracy is extremely important, these best EER values provide strong evidence that the method is capable of meeting stringent security requirements.

The effectiveness of this approach in handling passwords of different lengths and maintaining a relatively low and stable EER for different passwords is significant. This suggests that such a methodology can be applied to develop a versatile authentication system that is not only secure but also adaptable to natural changes in password lengths that occur in real-world cybersecurity scenarios.

For further experiments aimed at improving the performance of data fusion for training a single neural network for passwords of any length, three different experiments were designed, taking into account previous insights into the variability of performance with passphrase length:

- In the first experiment, the passphrases from the KeyRecs, CMU,

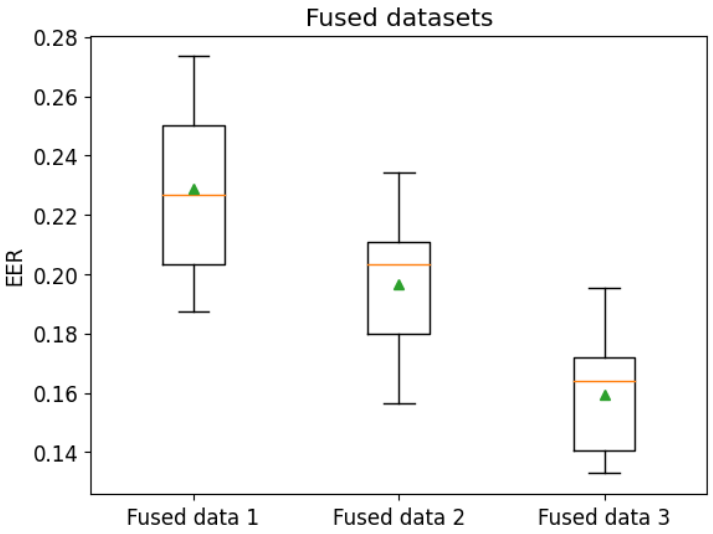


Figure 3.13: Comparison of EERs for fused keystroke dynamics datasets using different data fusion strategies, showing the impact on model accuracy and generalization to unseen data

Table 3.11: Performance metrics using the GREYC-NISLAB datasets using linear interpolation. The best, mean and standard deviations of EERs and accuracy values by specific passwords ("leonardo dicaprio", "michael schumacher", "red hot chilli peppers", "the rolling stones" and "united states of america") are presented, demonstrating the effectiveness of linear interpolation when dealing with passwords of different lengths

	Datasets				
Metrics	LDC	MS	RHCP	TRS	USA
Accuracy (best)	0.93750	0.96875	1.00000	0.96875	0.90625
Accuracy (mean)	0.87500	0.93229	0.87500	0.89583	0.83854
Accuracy (std)	0.03608	0.04199	0.06250	0.03898	0.04199
EER (best)	0.15625	0.15625	0.15625	0.1250	0.15625
EER (mean)	0.19792	0.18750	0.21354	0.17708	0.22396
EER (std)	0.02329	0.02552	0.04199	0.02946	0.03335

and GREYC-NISLAB datasets were fused into a single dataset to train SNN model. The trained model was then evaluated on an unseen subset of samples consisting of 15% of the users from each of these datasets. This combined dataset is referred to as "Fused data 1".

- The second experiment was designed to address the observed performance problems associated with longer passphrases. Here, the KeyRecs and GREYC-NISLAB datasets were fused, explicitly excluding the longer passphrases of RHCP and USA, as it was acknowledged that they had underperformed in previous analyses. The network was subsequently tested on the full CMU dataset. This combined dataset is referred to as "Fused data 2".

- In the third experiment, the fusion of the KeyRecs, CMU, and GREYC-NISLAB datasets also excluded the RHCP and USA passphrases, on the assumption that removing the longer passphrases might improve overall performance. This newly trained network was then tested with an unseen subset of 15% of the users from the CMU dataset, providing a reliable assessment of the model's generalizability. This combined dataset is referred to as "Fused data 3".

When analyzing "Fused data 1", which consists of passwords of various lengths, the best EER is 0.1875 (see Figure 3.13). Using "Fused data 2", there is a noticeable improvement in EER, suggesting that the elimination of long passwords may have had a positive impact on the model's performance. The use of "Fused data 3" achieves a lower mean EER and a narrower interquartile range. In particular, "Fused data 3" has the best EER value of 0.13281, demonstrating a remarkable level of accuracy in authenticating users. This shows robust and stable performance under different user data and indicates a successful improvement in the neural network's ability to generalize on unseen data.

This Section introduced a new authentication methodology that integrates keystroke dynamics with data fusion and deep learning techniques. In particular, it implements a standardized password length across multiple datasets for the first time, while leveraging a data fusion strategy to enhance the robustness of authentication systems. Given the unique objectives and experimental framework used, direct comparison

with previous studies is inherently limited, highlighting the uniqueness of the proposed approach. These results differ from those of other authors (see [5, 8, 56, 82, 91, 97]) because the aim was to standardize the number of password features to a commonly used length and train a single network suitable for all passwords. Although this approach is promising, especially in improving the generalizability of authentication systems for different user groups and is not dependent on password length, it is essential to consider how these results relate to existing research in this area.

3.7.2. Keystroke Dynamics Data Fusion Result Comparison with Previous Studies

The performance of keystroke biometrics is affected by variables such as emotional state, body posture, keyboard type, and other situational factors [72]. For some physiological biometrics, such as fingerprints or iris recognition, EER can range from 0.001 to 0.0077 [112]. However, for behavioral biometrics, EER can range from 0.1 to 0.2, which is often considered appropriate to ensure a balance between user experience and security measures [5, 8, 97]. This study and experiments present a methodology for user authentication based on keystroke dynamics, which differs in that the testing phase uses only data from new, unseen users. Unlike previous studies [56, 82, 91] in which the separation of training and test samples based on the same users could introduce bias and overestimate the results of performance evaluation, in the proposed model, performance was evaluated only on new, unseen users. By choosing different sets of users for training and testing, the results reflect the model's ability to generalize across different behaviors and typing patterns, which is important for real-world applications. This achievement is noteworthy given the inherent variability and complexity of biometric datasets, which often pose significant challenges for pattern recognition and anomaly detection systems. The methodology developed in this research provides a solid basis for improving neural network training to enhance the security and accuracy of biometric authentication systems.

Several studies have reported lower EERs than those observed in this thesis, requiring further discussion of the methodological differences and their implications for real-world applications. For example, in the study [82], using a CNN-based approach on the GREYC-NISLAB

dataset, the best obtained EER was approximately 0.05. However, it is important to note the methodological differences on which the obtained result depends. In this thesis, combining multiple passwords into a single long password consisting of 99 characters and 376 attributes makes it possible to obtain an extended set of features that affect the performance of the model. However, this approach cannot always be directly applied to real-world scenarios, where users typically enter shorter and fixed passwords. Conversely, this thesis employs a standardized approach, wherein the length of the password is set to 37 features. While this restricts the scope of the feature set, it enables a more pragmatic solution to user authentication.

Similar studies such as [33, 64] have demonstrated the effectiveness of random forest and support vector machine algorithms in keystroke dynamics, especially in scenarios with free-text input or long password phrases. These cases utilize a broader set of features available in free-text scenarios, improving the performance of the models. This work, by contrast, focuses on fixed-text authentication, where the feature set is restricted to a standard password length. This limitation, while challenging, is crucial for developing a generalized model that can handle a variety of user inputs without requiring significant customization for each use case.

3.7.3. Justification for Data Fusion

The use of data fusion in this thesis is motivated by the effort to create a single unified model capable of handling different types of passwords across a wide user database. Training separate models for each user or dataset is not only resource intensive, but also impractical for large-scale applications, especially in critical infrastructure where efficiency and scalability are crucial.

Data fusion approach, which combines multiple datasets into a standardized format, addresses these challenges by creating a more flexible model. This model can be generalized to different user profiles, making it applicable in real-world applications where users may have different typing behaviors. The slightly higher EER observed in this thesis reflects the rigorous testing conditions under which the model was evaluated on unseen data from new users, in contrast to some previous studies in which the testing was performed on validation data

from known users, potentially leading to lower EER due to overfitting.

The efficacy of the data fusion methodology on keystroke dynamics was subjected to rigorous examination through a series of experiments. The experiments demonstrate that the proposed system is capable of handling passwords of varying lengths by combining multiple datasets and standardizing the features through interpolation. The results demonstrate the significance of time series standardization and image resizing techniques in enhancing the precision and dependability of user authentication. A comparative analysis of EERs of the various merged datasets revealed a notable enhancement in the model's performance, particularly when longer passphrases were excluded, leading to a substantial reduction in EERs. This approach allows the development of a more generalizable model capable of authenticating users from diverse and previously unseen data, and demonstrates its potential in real-world applications where variability in password length and typing behavior can affect system reliability. Ultimately, the fusion-based methodology has demonstrated efficacy in addressing the challenges associated with keystroke dynamics, offering a more robust, scalable, and customizable authentication solution.

3.8. Conclusions of the Chapter

The chapter provides a comprehensive evaluation of the keystroke dynamics authentication system methodology, demonstrating its effectiveness through extensive experimentation on datasets such as CMU, GREYC-NISLAB, and KeyRecs. Transforming raw keystroke data into visual representations improves feature extraction and classification accuracy when integrated with SNN and CNN architectures. The method consistently achieves low EER, validating its robustness in real-world authentication scenarios.

GAFMAT outperforms conventional transformation techniques, including GADF, GASF, RP and MTF. Multidimensional embedding visualization further enhances the interpretability of the system, facilitating user behavior analysis and anomaly detection. The implementation of data fusion ensures adaptability to passwords of different lengths, confirming the scalability of the method.

Despite minor performance variations between password sets, the results demonstrate the ability of the proposed methodology to pro-

vide secure and reliable authentication in critical infrastructure environments. The thesis provides a foundation for further advances in biometric authentication, particularly in the refinement of data fusion and visualization strategies to improve system scalability and detection accuracy.

All results related to the testing of the proposed user authentication methodology, including the GAFMAT method, the design of the experiments, and the results described in this Chapter 2, have been previously presented at scientific conferences and published in peer-reviewed papers. The core user authentication methodology and the GAFMAT method were presented in [A.2]. The visualization methods used to evaluate and interpret the results are described in detail in [A.1]. In addition, data standardization and fusion methods have been published in [A.3], which have significantly improved the reliability of the authentication system. In addition, results related to the selection of the margin size in a Siamese neural network with a triplet loss function were presented and discussed in conference proceedings [B.2] and [B.1]. These publications generally confirm and validate the methodology and conclusions presented in this thesis.

This thesis proposes and validates a deep learning-based user authentication framework using keystroke dynamics, focusing on the detection of insider threats in critical infrastructure. The proposed methodology integrates non-image to image data transformation, data fusion strategies, and dimensionality reduction techniques to improve model performance, interpretability, and practical applicability.

The following conclusions summarize the key findings and contributions of this thesis:

- The proposed keystroke dynamics-based user authentication methodology was integrated with a deep learning approach, specifically Siamese neural networks with triplet loss, to differentiate between legitimate users and unauthorized access. The efficacy of the methodology in addressing insider threats within critical infrastructure systems was demonstrated using publicly available datasets.

- Transforming keystroke dynamics into images using GAFMAT improved feature extraction and model accuracy. Empirical results showed that GAFMAT-based image representations performed better than existing non-image to image methods (GASF, GADF, MTF, RP). On the CMU dataset, this method achieved an EER of 0.04545. In addition, in the GREYC-NISLAB dataset the EER ranged from 0.04444 to 0.07552. These results show that GAFMAT is effective in highlighting users' writing behavior, helping to distinguish users based on their writing styles.

- By utilizing specific interpolation-based data fusion strategies, as well as a Siamese neural network with a triplet loss function, the best equal error rate of 0.13281 was achieved for the unseen fused data from various publicly available data. This indicates that the proposed methodology can extend the capabilities of user authentication systems, thereby providing more robust security measures for critical infrastructures and insider detection.

- Dimensionality reduction methods for assessing SNN embeddings showed that SNN embeddings significantly improved the distinguishability of the users clusters compared to the raw data, with sil-

houette scores increasing from 0.23 to 0.52. This demonstrates that SNN with CNN branches effectively captures distinctive writing patterns, improving user distinction for authentication purposes.

[1] M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado, A. Davis, J. Dean, M. Devin, S. Ghemawat, I. Goodfellow, A. Harp, G. Irving, M. Isard, Y. Jia, R. Jozefowicz, L. Kaiser, M. Kudlur, J. Levenberg, D. Mané, R. Monga, S. Moore, D. Murray, C. Olah, M. Schuster, J. Shlens, B. Steiner, I. Sutskever, K. Talwar, P. Tucker, V. Vanhoucke, V. Vasudevan, F. Viégas, O. Vinyals, P. Warden, M. Wattenberg, M. Wicke, Y. Yu, and X. Zheng. TensorFlow: Large-scale machine learning on heterogeneous systems, 2015. URL `https://www.tensorflow.org/`. Software available from tensorflow.org.

[2] S. A. Abdulrahman and B. Alhayani. A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. *Materials Today: Proceedings*, 80:2642–2646, 2023.

[3] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen. Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. *IEEE Internet of Things Journal*, 8(1):65–84, 2020. doi: 10.1109/JIOT.2020.3020076.

[4] A. Acien, A. Morales, R. Vera-Rodriguez, J. Fierrez, and J. V. Monaco. Typenet: Scaling up keystroke biometrics. In *2020 IEEE International Joint Conference on Biometrics (IJCB)*, pages 1–7. IEEE, 2020. doi: 10.1109/IJCB48548.2020.9304908.

[5] A. Acien, A. Morales, J. V. Monaco, R. Vera-Rodriguez, and J. Fierrez. TypeNet: Deep learning keystroke biometrics. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 4(1):57–70, 2022. doi: 10.1109/TBIOM.2021.311254.

[6] M. N. Al-Mhiqani, R. Ahmad, Z. Z. Abidin, K. H. Abdulkareem, M. A. Mohammed, D. Gupta, and K. Shankar. A new intelligent multilayer framework for insider threat detection. *Computers & Electrical Engineering*, 97:107597, 2022.

[7] A. S. Alfoudi, M. R. Aziz, Z. A. A. Alyasseri, A. H. Alsaeedi, R. R. Nuiaa, M. A. Mohammed, K. H. Abdulkareem, and M. M. Jaber. Hyper clustering model for dynamic network intrusion detection. *IET Communications*, 2022.

[8] O. Alpar. Biometric keystroke barcoding: A next-gen authentication framework. *Expert Systems with Applications*, 177:114980, 2021. doi: 10.1016/j.eswa.2021.114980.

[9] J. Augutis, B. Jokšas, R. Krikštolaitis, and I. Žutautaitė. Criticality assessment of energy infrastructure. *Technological and economic development of economy*, 20(2):312–331, 2014. doi: 10.3846/20294913.2014.915245.

[10] B. Ayotte, M. Banavar, D. Hou, and S. Schuckers. Fast free-text authentication via instance-based keystroke dynamics. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2(4):377–387, 2020. doi: 10.1109/TBIOM.2020.3003988.

[11] A. H. Azizan, S. A. Mostafa, A. Mustapha, C. F. M. Foozy, M. H. A. Wahab, M. A. Mohammed, and B. A. Khalaf. A machine learning approach for improving the performance of network intrusion detection systems. *Annals of Emerging Technologies in Computing (AETiC)*, 5(5):201–208, 2021.

[12] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat. A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, 76:139–154, 2021.

[13] P. Bedi, N. Gupta, and V. Jindal. Siam-IDS: Handling class imbalance problem in intrusion detection systems using Siamese neural network. *Procedia Computer Science*, 171:780–789, 2020. doi: 10.1016/j.procs.2020.04.085.

[14] I. Borg and P. J. Groenen. *Modern multidimensional scaling: Theory and applications*. Springer Science & Business Media, New York, NY 100013, USA, 2005.

[15] J. Bromley, I. Guyon, Y. LeCun, E. Säckinger, and R. Shah. Signature verification using a "Siamese" time delay neural network. *Advances in neural information processing systems*, 6, 1993. doi: 10.1142/s0218001493000339.

[16] L. Bukauskas, A. Brilingaitė, A. Juozapavičius, D. Lepaitė, K. Ikamas, and R. Andrijauskaitė. Remapping cybersecurity competences in a small nation state. *Heliyon*, 9(1), 2023. doi: 10.1016/j.heliyon.2023.e12808.

[17] E. Carrizosa, A. V. Olivares-Nadal, and P. Ramírez-Cobo. Time series interpolation via global optimization of moments fitting. *European Journal of Operational Research*, 230(1):97–112, 2013. doi: 10.1016/j.ejor.2013.04.008.

[18] H. Çeker and S. Upadhyaya. Sensitivity analysis in keystroke dynamics using convolutional neural networks. In *2017 IEEE*

workshop on information forensics and security (WIFS), pages 1–6. IEEE, 2017. doi: 10.1109/WIFS.2017.8267667.

[19] N. C. S. Centre. Cyber threats to critical infrastructure in the Baltic sea region, 2024. URL `https://www.nksc.lt/doc/rkgc/2024_Cyber_Threats_to_Critical_Infrastructure_in_the_Baltic_Sea_region.pdf`.

[20] C.-B. Chen, H. Yang, and S. Kumara. Recurrence network modeling and analysis of spatial data. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 28(8), 2018. doi: 10.1063/1.5024917.

[21] D. Cheng, Y. Gong, S. Zhou, J. Wang, and N. Zheng. Person reidentification by multi-channel parts-based cnn with improved triplet loss function. In *Proceedings of the iEEE conference on computer vision and pattern recognition*, pages 1335–1344, 2016. doi: 10.1109/CVPR.2016.149.

[22] K. Cziner, E. Mutafungwa, J. Lucenius, and R. Järvinen. Critical information infrastructure protection in the Baltic sea area: The case of TETRA. *CIVPRO Working Paper, Helsinki University of Technology, Communications Laboratory*, 6, 2007.

[23] J. V. Di Nardo. Biometric technologies: functionality, emerging trends, and vulnerabilities. *Journal of Applied Security Research*, 4 (1-2):194–216, 2008.

[24] D. Dias, U. Dias, N. Menini, R. Lamparelli, G. Le Maire, and R. d. S. Torres. Image-based time series representations for pixelwise eucalyptus region classification: A comparative study. *IEEE Geoscience and Remote Sensing Letters*, 17(8):1450–1454, 2019. doi: 10.1109/LGRS.2019.2946951.

[25] D. Dias, A. Pinto, U. Dias, R. Lamparelli, G. Le Maire, and R. d. S. Torres. A multirepresentational fusion of time series for pixelwise classification. *IEEE journal of selected topics in applied earth observations and remote sensing*, 13:4399–4409, 2020. doi: 10.1109/JSTARS.2020.3012117.

[26] T. Dias, J. Vitorino, E. Maia, O. Sousa, and I. Praça. KeyRecs: A keystroke dynamics and typing pattern recognition dataset. *Data in Brief*, 50:109509, 2023. doi: 10.1016/j.dib.2023.109509.

[27] E. Dimara, A. Bezerianos, and P. Dragicevic. Conceptual and methodological issues in evaluating multidimensional visualizations for decision support. *IEEE Transactions on Visualization and*

Computer Graphics, 24(1):749–759, 2017. doi: 10.1109/TVCG.2017.2745138.

[28] S. Ding, L. Lin, G. Wang, and H. Chao. Deep feature learning with relative distance comparison for person re-identification. *Pattern Recognition*, 48(10):2993–3003, 2015. doi: 10.1016/j.patcog.2015.04.005.

[29] X. Dong and J. Shen. Triplet loss in Siamese network for object tracking. In *Proceedings of the European conference on computer vision (ECCV)*, pages 459–474, 2018. doi: 10.1007/978-3-030-01261-8_28.

[30] G. Dzemyda, O. Kurasova, and J. Žilinskas. *Multidimensional Data Visualization: Methods and Applications*, volume 75 of *Springer Optimization and its Applications*. Springer, New York, NY, 2013. doi: 10.1007/978-1-4419-0236-8.

[31] G. Dzemyda, M. Sabaliauskas, and V. Medvedev. Geometric MDS performance for large data dimensionality reduction and visualization. *Informatica*, 33(2):299–320, 2022. ISSN 0868-4952. doi: 10.15388/22-INFOR491.

[32] P. Editorial. How to choose the right angle for your press release, Jan. 2025. URL `https://presscloud.ai/en/pr-academy/how-to-choose-the-right-angle-for-your-press-release`. Accessed: 2025-04-22.

[33] K. Elliot, J. Graham, Y. Yassin, T. Ward, J. Caldwell, and T. Attie. A comparison of machine learning algorithms in keystroke dynamics. In *2019 international conference on computational science and computational intelligence (CSCI)*, pages 127–132. IEEE, 2019. doi: 10.1109/CSCI49370.2019.00028.

[34] M. Espadoto, R. M. Martins, A. Kerren, N. S. T. Hirata, and A. C. Telea. Toward a quantitative survey of dimension reduction techniques. *IEEE Transactions on Visualization and Computer Graphics*, 27(3):2153–2173, 2021. doi: 10.1109/TVCG.2019.2944182.

[35] A. Estebsari and R. Rajabi. Single residential load forecasting using deep learning and image encoding techniques. *Electronics*, 9(1):68, 2020. doi: 10.3390/electronics9010068.

[36] O. I. Falowo, J. Kropczynski, and C. Li. Protecting critical infrastructure: Strategies for managing cybersecurity risks in nuclear fusion facilities. In *2023 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable*

Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), pages 1050–1061. IEEE, 2023. doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom59178.2023.00170.

[37] Federal Bureau of Investigation. Internet crime report 2022. Available at https://www.ic3.gov/Media/PDF/AnnualReport/2022_-IC3Report.pdf, 2023.

[38] R. A. Fisher. Statistical methods for research workers. In S. Kotz and N. L. Johnson, editors, *Breakthroughs in Statistics: Methodology and Distribution*, pages 66–70. Springer New York, New York, NY, 1992. doi: 10.1007/978-1-4612-4380-9_6.

[39] T. Fujiwara, O.-H. Kwon, and K.-L. Ma. Supporting analysis of dimensionality reduction results with contrastive learning. *IEEE Transactions on Visualization and Computer Graphics*, 26(1):45–55, 2020. doi: 10.1109/TVCG.2019.2934251.

[40] A. M. Gedikli and M. Ö. Efe. A simple authentication method with multilayer feedforward neural network using keystroke dynamics. In *Pattern Recognition and Artificial Intelligence: Third Mediterranean Conference, MedPRAI 2019, Istanbul, Turkey, December 22–23, 2019, Proceedings 3*, pages 9–23. Springer, 2020. doi: 10.1007/978-3-030-37548-5_2.

[41] R. Giot, M. El-Abed, and C. Rosenberger. Greyc keystroke: a benchmark for keystroke dynamics biometric systems. In *2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, pages 1–6. IEEE, 2009. doi: 10.1109/BTAS.2009.5339051.

[42] A. Gnauck. Interpolation and approximation of water quality time series and process identification. *Analytical and bioanalytical chemistry*, 380:484–492, 2004. doi: 10.1007/s00216-004-2799-3.

[43] M. I. Gofman and M. Villa. Identity and war: The role of biometrics in the Russia-Ukraine crisis. *International Journal on Engineering, Science & Technology (IJonEST)*, 5(1), 2023.

[44] P. Grassi, M. Garcia, and J. Fenton. Digital identity guidelines. Technical report, National Institute of Standards and Technology, 2020.

[45] V. Gurčinas, J. Dautartas, J. Janulevičius, N. Goranin, and A. Čenys. A deep-learning-based approach to keystroke-injection payload

generation. *Electronics*, 12(13), 2023. ISSN 2079-9292. doi: 10.3390/electronics12132894. URL https://www.mdpi.com/2079-9292/12/13/2894.

[46] R. Hadsell, S. Chopra, and Y. LeCun. Dimensionality reduction by learning an invariant mapping. In *2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'06)*, volume 2, pages 1735–1742. IEEE, 2006. doi: 10.1109/CVPR.2006.100.

[47] I. Hazan, O. Margalit, and L. Rokach. Supporting unknown number of users in keystroke dynamics models. *Knowledge-Based Systems*, 221:106982, 2021. doi: 10.1016/j.knosys.2021.106982.

[48] A. Imamura and N. Arizumi. Gabor filter incorporated CNN for compression. In *2021 36th International Conference on Image and Vision Computing New Zealand (IVCNZ)*, pages 1–5. IEEE, 2021. doi: 10.1109/IVCNZ54163.2021.9653342.

[49] E. Ivannikova, G. David, and T. Hämäläinen. Anomaly detection approach to keystroke dynamics based user authentication. In *2017 IEEE Symposium on Computers and Communications (ISCC)*, pages 885–889. IEEE, 2017. doi: 10.1109/ISCC.2017.8024638.

[50] J. E. Jackson. *A user's guide to principal components*, volume 587. John Wiley & Sons, Hoboken, NJ, 1991. doi: 10.1002/0471725331.

[51] A. K. Jain and B. Gupta. A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, 16(4):527–565, 2022.

[52] H. Jmila, M. Ibn Khedher, G. Blanc, and M. A. El Yacoubi. Siamese network based feature learning for improved intrusion detection. In *International Conference on Neural Information Processing*, pages 377–389. Springer, 2019. doi: 10.1007/978-3-030-36708-4_31.

[53] I. Jolliffe. Principal component analysis, second edition. *Encyclopedia of Statistics in Behavioral Science*, 30, 2002. ISSN 00401706. doi: 10.2307/1270093.

[54] U. Juknevičiūtė and V. Murachov. Navigating the legal landscape of cybersecurity regulation in lithuania. *Teisės mokslo pavasaris 2024.*, pages 144–161, 2024. doi: 10.15388/TMP.2024.7.

[55] J.-K. Kamarainen, V. Kyrki, and H. Kalviainen. Invariance properties of Gabor filter-based features-overview and applications. *IEEE Transactions on image processing*, 15(5):1088–1099, 2006. doi:

10.1109/TIP.2005.864174.

[56] K. S. Killourhy and R. A. Maxion. Comparing anomaly-detection algorithms for keystroke dynamics. In *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*, pages 125–134. IEEE, 2009. doi: 10.1109/DSN.2009.5270346.

[57] G. J. Krishna, H. Jaiswal, P. S. R. Teja, and V. Ravi. Keystroke based user identification with XGBoost. In *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*, pages 1369–1374. IEEE, 2019. doi: 10.1109/TENCON.2019.8929453.

[58] O. Kurasova and A. Molyte. Quality of quantization and visualization of vectors obtained by neural gas and self-organizing map. *Informatica*, 22(1):115–134, 2011. ISSN 0868-4952. doi: 10.15388/informatica.2011.317.

[59] J. Leggett and G. Williams. Verifying identity via keystroke characterstics. *International Journal of Man-Machine Studies*, 28(1):67–76, 1988.

[60] M. Lepot, J.-B. Aubin, and F. H. Clemens. Interpolation in time series: An introductive overview of existing methods, their performance criteria and uncertainty assessment. *Water*, 9(10):796, 2017. doi: 10.3390/w9100796.

[61] K. Lis, E. Niewiadomska-Szynkiewicz, and K. Dziewulska. Siamese neural network for keystroke dynamics-based authentication on partial passwords. *Sensors*, 23(15):6685, 2023.

[62] M. Liu and J. Guan. User keystroke authentication based on convolutional neural network. In *Mobile Internet Security: Second International Symposium, MobiSec 2017, Jeju Island, Republic of Korea, October 19–22, 2017, Revised Selected Papers 2*, pages 157–168. Springer, 2019. doi: 10.1007/978-981-13-3732-1_13.

[63] S. Liu, W. Shao, T. Li, W. Xu, and L. Song. Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. *Digital Signal Processing*, 125:103120, 2022.

[64] A. Lo, V. H. Ayma, and J. Gutierrez-Cardenas. A comparison of authentication methods via keystroke dynamics. In *2020 IEEE Engineering International Research Conference (EIRCON)*, pages 1–4, 2020. doi: 10.1109/EIRCON51178.2020.9253751.

[65] X. Lu, S. Zhang, P. Hui, and P. Lio. Continuous authentication by free-text keystroke based on CNN and RNN. *Computers & Security*,

96:101861, 2020. doi: 10.1016/j.cose.2020.101861.

[66] S. Maheshwary, S. Ganguly, and V. Pudi. Deep secure: A fast and simple neural network based approach for user authentication and identification via keystroke dynamics. In *IWAISe: First International Workshop on Artificial Intelligence in Security*, volume 59, 2017.

[67] G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger, and J. Benjamin. Industrial and critical infrastructure security: Technical analysis of real-life security incidents. *Ieee Access*, 9:165295–165325, 2021. doi: 0.1109/ACCESS.2021.3133348.

[68] K. Mardia, J. Kent, and J. Bibby. *Multivariate analysis*. Probability and mathematical statistics. Acad. Press, London [u.a.], 1979. ISBN 0124712509. URL `http://gso.gbv.de/DB=2.1/CMD?ACT=SRCHA&SRT=YOP&IKT=1016&TRM=ppn+02434995X&sourceid=fbw_bibsonomy`.

[69] A. G. Martín, M. Beltrán, A. Fernández-Isabel, and I. M. de Diego. An approach to detect user behaviour anomalies within identity federations. *computers & security*, 108:102356, 2021. doi: 10.1016/j.cose.2021.102356.

[70] L. McInnes, J. Healy, N. Saul, and L. Großberger. UMAP: Uniform manifold approximation and projection. *Journal of Open Source Software*, 3(29):861, 2018. doi: https://doi.org/10.21105/joss.00861.

[71] I. Melekhov, J. Kannala, and E. Rahtu. Siamese network features for image matching. In *2016 23rd international conference on pattern recognition (ICPR)*, pages 378–383. IEEE, 2016.

[72] L. I. Millett and J. N. Pato. Biometric recognition: Challenges and opportunities. 2010. doi: 10.17226/12720.

[73] J. V. Monaco and M. M. Vindiola. Crossing domains with the inductive transfer encoder: Case study in keystroke biometrics. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–8. IEEE, 2016. doi: 10.1109/BTAS.2016.7791165.

[74] A. Morales, J. Fierrez, R. Tolosana, J. Ortega-Garcia, J. Galbally, M. Gomez-Barrero, A. Anjos, and S. Marcel. Keystroke biometrics ongoing competition. *IEEE Access*, 4:7736–7746, 2016. doi: 10.1109/ACCESS.2016.2626718.

[75] S. Moustakidis, N. I. Papandrianos, E. Christodolou, E. Papageorgiou, and D. Tsaopoulos. Dense neural networks in knee osteoarthritis classification: a study on accuracy and fairness. *Neural Computing and Applications*, pages 1–13, 2020. doi: 10.1007/s00521-020-05459-5.

[76] Y. Muliono, H. Ham, and D. Darmawan. Keystroke dynamic classification using machine learning for password authorization. *Procedia Computer Science*, 135:564–569, 2018. doi: 10.1016/j.procs.2018.08.209.

[77] K. P. Murphy. *Probabilistic machine learning: an introduction*. MIT press, Cambridge, Massachusetts, 2022.

[78] M. Nathan. Credential stuffing: new tools and stolen data drive continued attacks. *Computer Fraud & Security*, 2020(12):18–19, 2020. doi: 10.1016/S1361-3723(20)30130-5.

[79] National Cyber Security Centre (NCSC). Cyber essentials: Requirements for IT infrastructure v3.1. Available at https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf, 2023.

[80] M. Ondrašovič and P. Tarábek. Siamese visual object tracking: A survey. *IEEE Access*, 9:110149–110172, 2021. doi: 10.1109/ACCESS.2021.3101988.

[81] J. Orols, N. Kunicina, and R. Bruzgiene. Acquisition and processing of intelligent system control data for the analysis of the interdependence between critical infrastructures. In *2022 IEEE 63th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON)*, pages 1–6, 2022. doi: 10.1109/RTUCON56726.2022.9978775.

[82] Y. B. W. Piugie, J. Di Manno, C. Rosenberger, and C. Charrier. Keystroke dynamics based user authentication using deep learning neural networks. In *2022 International Conference on Cyberworlds (CW)*, pages 220–227. IEEE, 2022. doi: 10.1109/CW55638.2022.00052.

[83] A. Rahman, M. E. Chowdhury, A. Khandakar, A. M. Tahir, N. Ibtehaz, M. S. Hossain, S. Kiranyaz, J. Malik, H. Monawwar, and M. A. Kadir. Robust biometric system using session invariant multimodal eeg and keystroke dynamics by the ensemble of self-onns. *Computers in Biology and Medicine*, 142:105238, 2022.

[84] V. S. Rajkumar, A. Ştefanov, A. Presekal, P. Palensky, and J. L. R. Torres. Cyber attacks on power grids: Causes and propagation of cascading failures. *IEEE Access*, 11:103154–103176, 2023. doi: 10.1109/ACCESS.2023.3317695.

[85] P. Ray, S. S. Reddy, and T. Banerjee. Various dimension reduction techniques for high dimensional data analysis: a review. *Artificial Intelligence Review*, 54(5):3473–3515, 2021. doi: 10.1007/s10462-020-09928-0.

[86] S. T. Roweis and L. K. Saul. Nonlinear dimensionality reduction by locally linear embedding. *Science*, 290(5500):2323–2326, 2000.

[87] N. Sae-Bae and N. Memon. Distinguishability of keystroke dynamic template. *Plos one*, 17(1):e0261291, 2022. doi: 10.1371/journal.pone.0261291.

[88] M. Sandhya, M. K. Morampudi, I. Pruthweraaj, and P. S. Garepally. Multi-instance cancelable iris authentication system using triplet loss for deep learning models. *The Visual Computer*, pages 1–11, 2022. doi: 10.1007/s00371-022-02429-x.

[89] F. Schroff, D. Kalenichenko, and J. Philbin. Facenet: A unified embedding for face recognition and clustering. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 815–823, 2015. doi: 10.1109/CVPR.2015.7298682.

[90] A. Serwadda and V. V. Phoha. Examining a large keystroke biometrics dataset for statistical-attack openings. *ACM Transactions on Information and System Security (TISSEC)*, 16(2):1–30, 2013. doi: 10.1145/2516960.

[91] R. Shadman, A. A. Wahab, M. Manno, M. Lukaszewski, D. Hou, and F. Hussain. Keystroke dynamics: Concepts, techniques, and applications. *arXiv preprint arXiv:2303.04605*, 2023.

[92] A. Sharma, E. Vans, D. Shigemizu, K. A. Boroevich, and T. Tsunoda. DeepInsight: A methodology to transform a non-image data to an image for convolution neural network architecture. *Scientific reports*, 9(1):11399, 2019.

[93] K. Shekhawat and D. P. Bhatt. Recent advances and applications of keystroke dynamics. In *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, pages 680–683. IEEE, 2019. doi: 10.1109/ICCIKE47802.2019.9004312.

[94] M. Shutaywi and N. N. Kachouie. Silhouette analysis for per-

formance evaluation in machine learning with applications to clustering. *Entropy*, 23(6):759, 2021. doi: 10.3390/e23060759.

[95] A. I. Siam, A. Sedik, W. El-Shafai, A. A. Elazm, N. A. El-Bahnasawy, G. M. El Banby, A. A. Khalaf, and F. E. Abd El-Samie. Biosignal classification for human identification based on convolutional neural networks. *International journal of communication systems*, 34 (7):e4685, 2021. doi: 10.1002/dac.4685.

[96] R. Sibson. A brief description of natural neighbour interpolation. *Interpreting multivariate data*, pages 21–36, 1981.

[97] M. Singh and D. Pati. Replay attack detection using excitation source and system features. In *Advances in Ubiquitous Computing*, pages 17–44. Elsevier, 2020. doi: 10.1016/B978-0-12-816801-1.00002-5.

[98] S. Singh, A. Inamdar, A. Kore, and A. Pawar. Analysis of algorithms for user authentication using keystroke dynamics. In *2020 International Conference on Communication and Signal Processing (ICCSP)*, pages 0337–0341. IEEE, 2020. doi: 10.1109/ICCSP48568.2020.9182115.

[99] J. Soni and N. Prabakar. KeyNet: Enhancing cybersecurity with deep learning-based LSTM on keystroke dynamics for authentication. In J.-H. Kim, M. Singh, J. Khan, U. S. Tiwary, M. Sur, and D. Singh, editors, *Intelligent Human Computer Interaction*, pages 761–771, Cham, 2022. Springer International Publishing. ISBN 978-3-030-98404-5. doi: 10.1007/978-3-030-98404-5_67.

[100] V.-D. Stanciu, R. Spolaor, M. Conti, and C. Giuffrida. On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks. In *proceedings of the sixth ACM conference on data and application security and privacy*, pages 105–112, 2016. doi: 10.1145/2857705.2857748.

[101] C. O. Ugwuoke, O. J. Eze, S. O. Ameh, A. B. Mohammed, A. Linus, and A. Aroh. Armed robbery attacks and everyday life in Nigeria. *International journal of criminal justice sciences*, 16(1):186–200, 2021.

[102] J. J. Valero-Mas, A. J. Gallego, and J. R. Rico-Juan. An overview of ensemble and feature learning in few-shot image classification using siamese networks. *Multimedia Tools and Applications*, pages 1–24, 2023.

[103] L. Van der Maaten and G. Hinton. Visualizing data using t-SNE.

Journal of Machine Learning Research, 9(11):2579–2605, 2008.

[104] C. Ventures. Cybercrime to cost the world 8 trillion annually in 2023. *Cybersecurity Ventures*, 2023. URL https://www.cybersecurityventures.com.

[105] Verizon. 2023 Verizon data breach investigations report, 2023. URL https://www.verizon.com/business/resources/reports/dbir/. Accessed: 2023-09-06.

[106] Y. Wang, H. Huang, C. Rudin, and Y. Shaposhnik. Understanding how dimension reduction tools work: An empirical approach to deciphering t-SNE, UMAP, TriMap, and PaCMAP for data visualization. *Journal of Machine Learning Research*, 22(201):1–73, 2021.

[107] Z. Wang and T. Oates. Imaging time-series to improve classification and imputation. In *Proceedings of the 24th International Conference on Artificial Intelligence*, pages 3939–3945, 2015.

[108] M. Warkentin and R. Willison. Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2):101–105, 2009. doi: 10.1057/ejis.2009.12.

[109] I. William, E. H. Rachmawanto, H. A. Santoso, C. A. Sari, et al. Face recognition using facenet (survey, performance test, and comparison). In *2019 fourth international conference on informatics and computing (ICIC)*, pages 1–6. IEEE, 2019.

[110] X. Xu, T. Liang, J. Zhu, D. Zheng, and T. Sun. Review of classical dimensionality reduction and sample selection methods for large-scale data processing. *Neurocomputing*, 328:5–15, 2019. doi: 10.1016/j.neucom.2018.02.100.

[111] C. Yan, G. Pang, X. Bai, C. Liu, X. Ning, L. Gu, and J. Zhou. Beyond triplet loss: person re-identification with fine-grained difference-aware pairwise loss. *IEEE Transactions on Multimedia*, 24:1665–1677, 2021. doi: 10.1109/TMM.2021.3069562.

[112] T. Yoshida and S. Hangai. A study on accuracy and problems in using ISO/IEC 19794-2 finger minutiae formats for automated fingerprint verification, 2010. URL https://www.nist.gov/system/files/documents/2022/02/17/yoshida2_takahiro_paper.pdf. Accessed: 2025-04-22.

[113] D. Zaidan, A. Salem, A. Swidan, and R. Saifan. Factors affecting

keystroke dynamics for verification data collecting and analysis. In *2017 8th International Conference on Information Technology (ICIT)*, pages 392–398. IEEE, 2017. doi: 10.1109/ICITECH.2017.8080032.

[114] Y. Zhang, Y. Hou, S. Zhou, and K. Ouyang. Encoding time series as multi-scale signed recurrence plots for classification using fully convolutional networks. *Sensors*, 20(14):3818, 2020. doi: 10.3390/s20143818.

[115] X. Zhao, H. Sun, B. Lin, H. Zhao, Y. Niu, X. Zhong, Y. Wang, Y. Zhao, F. Meng, J. Ding, X. Zhang, L. Dong, and S. Liang. Markov transition fields and deep learning-based event-classification and vibration-frequency measurement for ϕ-otdr. *IEEE Sensors Journal*, 22(4):3348–3357, 2022. doi: 10.1109/JSEN.2021.3137006.

[116] Y. Zhong, Y. Deng, and A. K. Jain. Keystroke dynamics for user authentication. In *2012 IEEE computer society conference on computer vision and pattern recognition workshops*, pages 117–123. IEEE, 2012. doi: 10.1109/CVPRW.2012.6239225.

[117] X. Zhou, W. Liang, S. Shimizu, J. Ma, and Q. Jin. Siamese neural network based few-shot learning for anomaly detection in industrial cyber-physical systems. *IEEE Transactions on Industrial Informatics*, 17(8):5790–5798, 2020. doi: 10.1109/TII.2020.3047675.

[118] Z.-H. Zhou. Dimensionality reduction and metric learning. In *Machine Learning*, pages 241–264. Springer, Singapore, 2021. doi: https://doi.org/10.1007/978-981-15-1967-3_10.

[119] Y. Zhu, T. Brettin, F. Xia, A. Partin, M. Shukla, H. Yoo, Y. A. Evrard, J. H. Doroshow, and R. L. Stevens. Converting tabular data into images for deep learning with convolutional neural networks. *Scientific reports*, 11(1):11325, 2021. doi: 10.1038/s41598-021-90923-y.

Articles published in international research journals with a citation index in the Clarivate Web of Science (WoS) database:

[A.1] O. Kurasova, A. Budžys & V. Medvedev. Exploring multidimensional embeddings for decision support using advanced visualization techniques. *Informatics*. Basel: MDPI, 2024, **vol. 11**, iss. 1, art. no. 11, pp. 1–17. eISSN 2227-9709. doi: 10.3390/informatics11010011 [Emerging Sources Citation Index (Web of Science); Scopus] [IF: 3,400; Q2 (2023, InCites JCR ESCI)].

[A.2] A. Budžys, O. Kurasova & V. Medvedev (2024). Deep learning-based authentication for insider threat detection in critical infrastructure. *Artificial intelligence review*. Dordrecht: Springer Nature B.V., 2024, **vol. 57**, iss. 10, art. no. 272, pp. 1–35. ISSN 0269-2821. eISSN 1573-7462. doi: 10.1007/s10462-024-10893-1 [Science Citation Index Expanded (Web of Science)] [IF: 10,700; Q1 (2023, InCites JCR SCIE)].

[A.3] A. Budžys, O. Kurasova & V. Medvedev (2024). Integrating Deep Learning and Data Fusion for Advanced Keystroke Dynamics Authentication. *Computer Standards & Interfaces*. Amsterdam: Elsevier B.V., 2024, **vol. 92**, art. no. 103931, pp. 1–14. ISSN 0920-5489. doi: 10.1016/j.csi.2024.103931. [Science Citation Index Expanded (Web of Science); Scopus] [IF: 4.100; Q1 (2023, InCites JCR SCIE)].

Papers in peer-reviewed scientific conference proceedings:

[B.1] V. Medvedev, A. Budžys & O. Kurasova. Enhancing keystroke biometric authentication using deep learning techniques. In: 2023 18th Iberian Conference on Information Systems and Technologies (CISTI), 20-23 June, Aveiro, Portugal, 2023: proceedings. New York: IEEE, 2023, pp. 1–6. ISSN 2166-0727. eISSN 2166-0727. ISBN 9798350305272. eISBN 9789893347928. doi: 10.23919/CISTI58278.2023.10211344.

[B.2] A. Budžys, O. Kurasova & V. Medvedev. Behavioral biometrics authentication in critical infrastructure using siamese neural networks. In: HCI for cybersecurity, privacy and trust: 5th international conference, HCI-CPT 2023, held as part of the 25th HCI

international conference, HCII 2023. Copenhagen, Denmark, July 23–28, 2023: proceedings. Cham: Springer, 2023, pp. 309-322. Lecture notes in computer science, vol. 14045. ISBN 9783031358210. eISBN 9783031358227. doi: 10.1007/978-3-031-35822-7_21.

Papers in national scientific conference proceedings:

[C.1] V. Medvedev, A. Budžys & O. Kurasova. User behaviour analysis based on similarity measures to detect anomalies // DAMSS: 12th conference on data analysis methods for software systems, Druskininkai, Lithuania, December 2–4, 2021. Vilnius : Vilnius University Press, 2021. ISBN 9786090706732. eISBN 9786090706749. p. 8. DOI: 10.15388/DAMSS.12.2021.

[C.2] A. Budžys, O. Kurasova & V. Medvedev. Deep learning-based prevention of insider threats using user behavioral keystroke biometrics // *EURO 2022: [32nd European Conference on Operational Research (EURO XXXII)], Espoo, Finland, July 3–6, 2022* : abstract book. Espoo : Aalto university, 2022. ISBN 9789519525419. p. 144. Prieiga per internetą: <https://www.euro-online.org/conf/admin/tmp/program-euro32.pdf>.

[C.3] A. Budžys, O. Kurasova & V. Medvedev. Intrusion detection based on keystroke biometrics and siamese neural networks // *DAMSS: 13th conference on data analysis methods for software systems, Druskininkai, Lithuania, December 1–3, 2022*. Vilnius : Vilnius University Press, 2022. ISBN 9786090707944. eISBN 9786090707951. p. 13. (Vilnius University Proceedings, eISSN 2669-0233 ; vol. 31). DOI: 10.15388/DAMSS.13.2022.

[C.4] A. Budžys, O. Kurasova & V. Medvedev. Insider threat detection: a new keystroke dynamics-based approach to user authentication in critical infrastructure // *DAMSS: 14th conference on data analysis methods for software systems, Druskininkai, Lithuania, November 30–December 2, 2023*. Vilnius. Vilnius : Vilniaus universiteto leidykla, 2023. eISBN 9786090709856. p. 16. (Vilnius University Proceedings, eISSN 2669-0233 ; vol. 39). DOI: 10.15388/DAMSS.14.2023.

[C.5] V. Medvedev, A. Budžys & O. Kurasova. Enhancing cybersecurity using keystroke dynamics and data fusion techniques // *DAMSS: 15th conference on data analysis methods for software systems, Druskininkai, Lithuania, November 28-30, 2024*. Vilnius : Vilniaus universiteto leidykla, 2024. eISBN 9786090711125. p. 14. (Vilnius University Proceedings, eISSN 2669-0233 ; vol. 52). DOI: 10.15388/DAMSS.15.2024.

CURRICULUM VITAE

Arnoldas Budžys was born on April 12, 1985, in Lithuania. He obtained his Master's degree in Informatics from Vilnius University, Faculty of Mathematics and Informatics, in 2020. Since 2020, he has been pursuing a PhD at the Vilnius University Institute of Data Science and Digital Technologies, focusing on cybersecurity, machine learning, and biometric authentication based on keystroke dynamics. He works as a cybersecurity engineer. His research interests include cybersecurity, anomaly detection, deep learning, and behavioral biometrics. He actively participates in international conferences and cybersecurity exercises.

Šiuolaikinė skaitmeninė aplinka suteikia kibernetiniams nusikaltėliams plačias galimybes atakuoti nacionalinius tinklus ir ypatingos svarbos infrastruktūrą, pavyzdžiui, reikalauti išpirkos už duomenis, vykdyti plataus masto sukčiavimą ar kelti grėsmę nacionaliniam saugumui. Šių grėsmių pasekmės gali būti skaudžios – nuo didelių finansinių nuostolių iki reputacijos žalos ir klientų pasitikėjimo praradimo. Kibernetinio saugumo iššūkiai vystosi taip greitai, kad tradiciniai, slaptažodžiais grįsti autentifikavimo metodai tampa vis mažiau veiksmingi. Nors slaptažodžiai vis dar plačiausiai naudojami, jie dažnai tampa „phishing“, „brute force“, socialinės inžinerijos ar vidinių grėsmių taikiniais, sukeliančiais duomenų saugumo pažeidimus ir finansinius nuostolius. Šios problemos aktualios ypatingos svarbos infrastruktūros sektoriams, tokiems kaip energetika, transportas, sveikatos priežiūra, finansai ir gynyba. Kai nusikaltėliai įgyja neteisėtą prieigą prie tokių sistemų, pasekmės gali būti kur kas rimtesnės nei vien finansiniai nuostoliai – gali sutrikti esminių paslaugų teikimas ir kilti grėsmė valstybės saugumui [36, 84].

Pavogti prisijungimo duomenys sudaro net 80 % finansinių nuostolių, susijusių su kibernetiniais nusikaltimais [105]. „Phishing“ – tai kibernetinės atakos forma, kai naudojantis apgaulingais el. laiškais, SMS žinutėmis ar telefono skambučiais, apsimetant patikima institucija, iš neatsargių gavėjų išgaunama asmeninė informacija [12, 51]. Siekiant apsisaugoti nuo tokių grėsmių, rekomenduojama naudoti daugiafaktorinį autentifikavimą. Tačiau net ir jis gali būti pažeidžiamas tuo atveju, kai slaptažodžiai yra silpni, pakartotinai naudojami ar jau nutekėję. Neseniai paskelbta ataskaita rodo, kad silpni ar pažeisti slaptažodžiai sudaro didelę dalį nutekėjusių duomenų, o tai dar kartą pabrėžia papildomų apsaugos priemonių svarbą [37, 105].

Elgsenos biometrija yra veiksminga antroji gynybos linija. Vienas iš jos pavyzdžių – klavišų paspaudimo dinamika, kuri leidžia nustatyti naudotojo tapatybę analizuojant subtilius įvesties aspektus, tokius kaip spausdinimo ritmas, laiko intervalai ir paspaudimo stiprumas, nereikalaujant papildomos techninės įrangos. Šis metodas fiksuoja įvairius naudotojo spausdinimo elgsenos bruožus – klavišų paspaudimo ir atleidimo laiką, spausdinimo greitį bei ritmą. Analizuojant šiuos duomenis, sukuriamas unikalus biometrinis profilis, kuris gali būti naudojamas nuolatiniam naudotojo autentifikavimui. Tai leidžia efektyviai aptikti ir

užkirsti kelią neteisėtai prieigai prie svarbių sistemų ir duomenų.

Nepaisant akivaizdžių privalumų, klavišų paspaudimo dinamika susiduria ir su iššūkiais. Vienas pagrindinių – didelis duomenų kintamumas, kylantis dėl rašymo stiliaus svyravimų, kuriuos gali lemti stresas, naudotojo laikysena ar aplinkos sąlygos. Be to, taikant šį metodą būtina atsižvelgti į skirtingus slaptažodžius, įvairias naudotojų grupes ir realaus laiko autentifikavimo sąlygas, išvengiant perteklinio klaidingai teigiamų ar klaidingai neigiamų atvejų skaičiaus.

Naujausi giliojo mokymosi pasiekimai gerokai išplėtė galimybes analizuoti sudėtingas naudotojų savybes klavišų paspaudimų duomenyse. Skirtingai nei tradiciniai mašininio mokymosi metodai, kurie dažnai remiasi rankiniu būdu išgautais požymiais ir sunkiai aptinka sudėtingus raštus, giliojo mokymosi architektūros geba automatiškai identifikuoti subtilius laiko ir erdvės požymius.

Disertacijoje daugiausia dėmesio skiriama statiniam autentifikavimui, kai naudotojai turi įvesti slaptažodžius jiems būdingu rašymo stiliumi. Nors nuolatinio autentifikavimo metodai turi savų privalumų, statiniai metodai vis dar plačiai taikomi kritinėse sistemose. Be to, jie leidžia tiesiogiai lyginti rezultatus su ankstesniais tyrimais naudojant standartinius kokybės rodiklius, tokius kaip vienodas klaidų santykis (angl. *Equal Error Rate*, toliau EER) [56].

Sujungus giliojo mokymosi modelius, duomenų transformaciją į vaizdus ir patikimas suliejimo strategijas, šiame darbe siekiama parodyti, kaip autentifikavimo sistema efektyviai prisitaiko prie skirtingų naudotojų ir slaptažodžių, taip stiprinant ypatingos svarbos infrastruktūros saugumą.

Šio darbo **tikslas** – sukurti ir įvertinti giliuoju mokymusi pagrįstą metodiką, skirtą vidinėms grėsmėms ypatingos svarbos infrastruktūros sistemose aptikti. Šia metodika siekiama pagerinti vidinių grėsmių ir neleistinos prieigos aptikimą, transformuojant nevaizdinius arba lentelėse pateiktus klavišų paspaudimų duomenis į vaizdinius atvaizdus. Joje taip pat pateikiamas naujas požiūris į naudotojo autentifikavimą, grindžiamą klavišų paspaudimų dinamika, naudojant Siamo neuroninio tinklo architektūrą su konvoliucinio neuroninio tinklo atšakomis.

Norint pasiekti šio darbo tikslus, reikia įgyvendinti šiuos **uždavinius**:

1. Atlikti išsamią literatūros apžvalgą apie ypatingos svarbos inf-

rastruktūrose naudojamus naudotojų autentiškumo patvirtinimo metodus, ypatingą dėmesį skiriant elgsenos biometrijai, ypač klavišų paspaudimo dinamikai.

2. Įvertinti giliojo mokymosi metodus ir kokybės vertinimo metrikas, skirtas vidinėms grėsmėms aptikti analizuojant klavišų paspaudimų elgseną, ir nustatyti jų poveikį naudotojo autentiškumo nustatymo tikslumui didinti.

3. Pasiūlyti naują naudotojo autentiškumo nustatymo metodiką, pagrįstą klavišų paspaudimų dinamika, naudojant elgsenos biometrijos ir giliojo mokymosi metodų įžvalgas ir sujungiant kelis skirtingo ilgio slaptažodžius, siekiant pagerinti grėsmių aptikimą.

4. Įvertinti siūlomos metodikos veiksmingumą naudojant viešai prieinamus klavišų paspaudimų dinamikos duomenų rinkinius.

Mokslinis darbo naujumas

Šioje disertacijoje pristatomi keli nauji indėliai į naudotojų autentifikavimo ir kibernetinio saugumo sritis. Ypatingas dėmesys skiriamas vidinių grėsmių aptikimui ypatingos svarbos infrastruktūros sistemose, pasitelkiant klavišų paspaudimų dinamiką ir giliojo mokymosi metodus.

Pagrindinis šio darbo privalumas – sukurta ir įvertinta giliojo mokymosi metodika, skirta vidinių grėsmių identifikavimui ypatingos svarbos infrastruktūros sistemose. Metodika pagrįsta nevaizdinių klavišų paspaudimų dinamikos duomenų transformacija į vaizdus, pasitelkiant naują Gaboro filtro matricos transformacijos metodą (angl. *GAbor Filter MAtrix Transformation*, toliau GAFMAT). Ši transformacija leidžia išnaudoti Siamo neuroninių tinklų (angl. *Siamese Neural Network*, toliau SNN) architektūrą, kurioje integruoti konvoliuciniai neuroniniai tinklai (angl. *Convolutional Neural Network*, toliau CNN).

Be to, metodikoje pateiktas sprendimas, kaip standartizuoti klavišų paspaudimų dinamikos duomenis skirtingo ilgio slaptažodžiams, taikant interpoliacijos ir vaizdo dydžio keitimo metodus. Duomenų suliejimo strategijų taikymas padeda modeliams geriau apibendrinti įvesties duomenis, nepriklausomai nuo slaptažodžio ilgio.

Taigi, ši metodika siūlo vaizdais grįstą naudotojų autentifikavimo sprendimą, paremtą elgsenos biometrija, kuris leidžia efektyviau aptikti

vidines grėsmes bei neteisėtą prieigą prie svarbių sistemų.

Pagrindinis tyrimo naujumas:

1. Pristatomas naujas duomenų transformacijos metodas GAFMAT, skirtas klavišų paspaudimo dinamikos požymių išskyrimui pagerinti ir naudotojo autentiškumo nustatymui naudojant SNN su CNN atšakomis.

2. Sukurtas klavišų paspaudimų dinamikos standartizavimo sprendimas, kuriuo siekiama pašalinti duomenų rinkinių įvairovę naudojant duomenų sujungimo, interpoliavimo ir vaizdo dydžio keitimo metodus.

3. Siūloma kompleksinė naudotojo autentifikavimo sistema, kurioje GAFMAT integruojamas su giliojo mokymosi metodais, skirta vidinėms grėsmėms aptikti ypatingos svarbos infrastruktūroje, naudojant biometrinių duomenų elgsenos analizę.

Ginamieji teiginiai

Šios disertacijos ginamieji teiginiai:

1. Klavišų paspaudimo dinamikos duomenų transformavimas į vaizdus, pasitelkiant naują metodą GAFMAT, padidina giliojo mokymosi modelio efektyvumą naudotojų autentifikavime. Standartizavus klavišų paspaudimo duomenis ir taikant šį transformavimo metodą, sistema geriau atskiria teisėtus naudotojus nuo apsimetėlių.

2. Tyrimas, kurio metu buvo taikytos dvi duomenų standartizavimo strategijos – laiko eilučių interpoliacija ir vaizdų dydžio keitimas su interpoliacija, atskleidė, kad tiesinė interpoliacija užtikrina mažiausią vidutinį vienodą klaidų santykį bei stabilų veikimą įvairiuose duomenų rinkiniuose.

3. Siūloma naudotojų autentifikavimo metodika skirta praktiniam taikymui realioje kritinės infrastruktūros aplinkoje. Ji buvo įvertinta eksperimentiniais tyrimais, naudojant viešai prieinamus duomenų rinkinius, kurie parodė šio metodo pritaikomumą, universalumą ir veiksmingumą naudotojų autentifikavimui.

Mokslinių rezultatų aprobavimas

Tyrimų rezultatai paskelbti 5 moksliniuose straipsniuose: 3 straipsniai periodiniuose mokslo žurnaluose, indeksuojamuose Clarivate Web of Science (WoS); 2 straipsniai recenzuojamuose mokslinių konferencijų leidiniuose, bei pristatyti 2 tarptautinėse ir 4 nacionalinėse mokslinėse konferencijose.

Straipsniai WoS duomenų bazės leidiniuose:

1. Budžys, Arnoldas; Kurasova, Olga; Medvedev, Viktor. Deep Learning-Based Authentication for Insider Threat Detection in Critical Infrastructure // *Artificial Intelligence Review*. Dordrecht : Springer Nature B.V. ISSN 0269-2821. eISSN 1573-7462. 2024, vol. 57, iss. 10, art. no. 272, p. 1–35. DOI: 10.1007/s10462-024-10893-1.

2. Budžys, Arnoldas; Medvedev, Viktor; Kurasova, Olga. Integrating Deep Learning and Data Fusion for Advanced Keystroke Dynamics Authentication // *Computer Standards & Interfaces*. Amsterdam : Elsevier B.V. ISSN 0920-5489. 2025, vol. 92, art. no. 103931, p. 1–14. DOI: 10.1016/j.csi.2024.103931.

3. Kurasova, Olga; Budžys, Arnoldas; Medvedev, Viktor. Exploring Multidimensional Embeddings for Decision Support Using Advanced Visualization Techniques // *Informatics*. Basel : MDPI. eISSN 2227-9709. 2024, vol. 11, iss. 1, art. no. 11, p. 1–17. DOI: 10.3390/informatics11010011.

Pranešimai tarptautinėse mokslinėse konferencijose:

1. Budžys, Arnoldas. Deep Learning-Based Prevention of Insider Threats Using User Behavioral Keystroke Biometrics. EURO 2022: 32nd European Conference on Operational Research (EURO XXXII), Espoo, Finland, July 3–6, 2022.

2. Budžys, Arnoldas. Behavioral Biometrics Authentication in Critical Infrastructure Using Siamese Neural Networks. HCI for Cybersecurity, Privacy and Trust: 5th international conference, HCI-CPT 2023, held as part of the 25th HCI international conference, HCII 2023. Copenhagen, Denmark, July 23–28, 2023.

Disertacijos struktūra

Šią disertaciją sudaro trys pagrindiniai skyriai, po kurių pateikiamos bendrosios išvados ir literatūros sąrašas.

- Pirmame skyriuje pateikiama išsami literatūros apžvalga, kurioje daugiausia dėmesio skiriama mašininio mokymosi metodams, susijusiems su klavišų paspaudimų dinamika, įskaitant SNN, duomenų standartizavimą ir daugiamačių duomenų vizualizavimo metodus.
- Antrame skyriuje pateikiama naudotojo autentiškumo nustatymo metodika, daugiausia dėmesio skiriant SNN architektūrai, klavišų paspaudimų skaitinių duomenų transformacijai į vaizdus taikant GAFMAT.
- Trečiame skyriuje pateikiami eksperimentai ir jų rezultatai, gauti taikant pasiūlytą metodiką.
- Galiausiai, bendrųjų išvadų skyriuje apibendrinamos pagrindinės tyrimo išvados, po kurių pateikiama išsami bibliografija.

Lietuvišką santrauką sudaro 25 puslapiai, kurioje yra 5 paveikslai ir 6 lentelės.

S.1. LITERATŪROS APŽVALGA

Svarbiausių infrastruktūrų, tokių kaip elektros tinklai, transporto ir ryšių sistemos, saugumas yra gyvybiškai svarbus visuomenės stabilumui užtikrinti. Dėl to augančios kibernetinės grėsmės gali turėti itin neigiamų pasekmių. Tradicinės slaptažodžiais grindžiamos autentifikavimo priemonės dažnai yra pažeidžiamos kibernetinių atakų, kurių metu pasisavinami prisijungimo duomenys [78]. Ypatingos svarbos infrastruktūros sistemoms taip pat kyla didelė rizika dėl vidinių grėsmių, kai autorizuoti naudotojai, neteisėtai pasinaudoję kitų prisijungimo duomenimis, sukelia įvairius saugumo pažeidimus [67, 108].

Vidinės grėsmės dažnai siejamos su asmenimis, turinčiais teisėtą prieigą prie sistemų ir gerai išmanančiais jų vidinius procesus [108]. Lietuvoje taip pat vykdomi aktyvūs tyrimai, susiję su ypatingos svarbos infrastruktūros apsauga [9, 45, 81]. Įvairios kibernetinio saugumo pratybos, tokios kaip „Locked Shields“, rodo vis didėjantį poreikį taikyti sudėtingesnius saugumo sprendimus [19, 22].

Nesankcionuoti prisijungimai, naudojant pavogtus prisijungimo duomenis, jau ilgą laiką išlieka vienu pagrindinių būdų įsilaužti į informacines sistemas [37, 104, 105]. Siekiant sumažinti tokių grėsmių riziką, kuriamos stebėjimo ir reagavimo sistemos, skirtos tinklų ir sistemų veiklai analizuoti [6, 7, 11]. Tačiau, didėjant atakų sudėtingumui, vis dažniau diegiami daugiafaktoriniai autentifikavimo sprendimai, į kuriuos įtraukiami fiziologiniai arba elgsenos biometrijos duomenys [2, 43, 101]. Tyrimai rodo, kad klaviatūros dinamikos analizė gali sustiprinti naudotojo autentifikavimą, nes remiasi individualiais spausdinimo įpročiais, kuriuos yra sudėtinga atkartoti [59].

Klaviatūros dinamika gali būti taikoma tiek statiniam, tiek nuolatiniam naudotojo autentiškumo nustatymui [23]. Vienas pagrindinių šio metodo efektyvumo rodiklių yra vienodas klaidų santykis (EER). Siekiant patikimumo, EER reikšmė turėtų būti kuo artimesnė nuliui [40, 41, 56, 93, 98, 113]. Kaip pabrėžia [99] autoriai, diegiant tokius sprendimus praktikoje, svarbu išlaikyti tinkamą pusiausvyrą tarp naudotojo patogumo ir sistemos saugumo.

Lietuvoje daug dėmesio skiriama tiek kritinės infrastruktūros apsaugai, tiek elgsenos biometrijos sprendimų plėtrai [9, 45, 81]. Didėjant kibernetinių atakų sudėtingumui, tampa vis svarbiau kurti priemones,

padedančias atpažinti klaviatūros injekcijas ir kitus įsilaužimo būdus, kurie imituoja teisėto naudotojo veiksmus [19, 45]. Nacionalinio kibernetinio saugumo centro ataskaitose pažymima, kad elgsenos analizė kartu su dirbtiniu intelektu gali padėti operatyviai reaguoti į grėsmes ir prireikus automatiškai jas neutralizuoti [19].

Apibendrinant galima teigti, kad statinės klaviatūros biometrijos metodai, taikomi naudotojo prisijungimo metu įvedant autentifikavimo duomenis, turi pasižymėti mažu EER, siekiant užtikrinti patikimą ir patogų tapatybės nustatymo procesą. Tik pasiekus pakankamą statinio autentifikavimo tikslumą galima svarstyti nuolatinio autentifikavimo sprendimų diegimą. Priešingu atveju papildomos saugumo priemonės gali būti neveiksmingos, jei pradinis autentifikavimo etapas išliks pažeidžiamas ir sudarys galimybes neautorizuotai prieigai.

S.1.1. Mašininis mokymasis klaviatūros paspaudimų dinamikoje

Tyrimai rodo, kad EER galima sumažinti pritaikius skirtingus atstumo skaičiavimo metodus [49, 73, 87, 116]. Tačiau realiose situacijose naudotojo rašymui įtakos turi fizinė būklė, emocijos, todėl kai kurie tyrimai gali būti pernelyg optimistiški. Dažniausiai naudojami viešai prieinami duomenų rinkiniai yra CMU [56], GREYC-NISLAB [41] ir KeyRecs [26].

Šie duomenų rinkiniai naudojami statinio autentifikavimo modelių tikslumui įvertinti, o jų išsamesnis palyginimas pateiktas S.1 lentelėje.

Pastaraisiais metais klaviatūros biometrijos srityje vis daugiau dėmesio skiriama giliojo mokymosi modelių taikymui, siekiant pritaikyti autentifikavimo sistemas prie skirtingų naudotojų rašymo ypatybių. Vienas iš perspektyviausių sprendimų yra SNN taikymas [80, 117]. Šie tinklai, sudaryti iš dviejų identiškų potinklių, vertina dviejų įvesties pavyzdžių panašumą, todėl tinka tapatybės nustatymo užduotims.

Siamo tinklai leidžia identifikuoti subtilius skirtumus tarp teisėtų naudotojų ir galimų užpuolikų, o tai itin reikšminga kibernetinio saugumo kontekste. Tyrimai rodo, kad SNN efektyvumą pagerina trejetų nuostolių funkcija (angl. *triplet loss function*), kuri priartina panašias įvestis ir atitolina nepanašias [46, 89]. Tokios funkcijos itin svarbios siekiant tiksliai atskirti rašymo modelius, esant reikšmingiems duomenų skirtumams, būdingiems įsilaužimų aptikimo sistemoms [13, 52, 75].

Kai kuriose srityse skaitmeninius duomenis būtina paversti vaizdais,

S.1 lentelė: Lyginamoji klavišų paspaudimų dinamikos ir autentifikavimo sistemų kibernetinio saugumo srityje analizė

Šaltinis	Metodika	Duomenų rinkinys	Saugumo sritis	Aut. metodas	Taikytos metrikos
[56]	anomalijų aptikimo algoritmai, atstumo funkcijos	CMU	klaviatūros dinamika	statinis	EER
[116]	atstumo funkcijos	CMU	klaviatūros dinamika	statinis	EER
[73]	indukcinis perdavimo enkoderis	CMU	klaviatūros dinamika	statinis	EER
[18]	CNN	CMU, GREYC-NISLAB	klaviatūros dinamika	statinis	EER
[49]	k-NN	CMU	klaviatūros dinamika	statinis	EER
[76]	mašininis mokymasis	CMU	klaviatūros dinamika	statinis	Tikslumas
[57]	XGBoost	CMU	klaviatūros dinamika	statinis	Tikslumas
[62]	CNN	CMU	klaviatūros dinamika	statinis	FAR, Tikslumas
[10]	egzemplioriais pagrįsti algoritmai	Clarkson II, Buffalo	klaviatūros dinamika, įsibrovimo aptikimas	dinaminis	EER
[3]	elgsenos biometrija	biometriniai rinkiniai	elgsenos biometrijos	dinaminis	EER, FAR, FRR
[65]	CNN, RNN	Clarkson II, Buffalo	klaviatūros dinamika	dinaminis	EER
[98]	XGBoost	CMU	klaviatūros dinamika	statinis	Tikslumas
[4]	Siamo RNN	Aalto	klaviatūros dinamika	dinaminis	EER
[11]	mašininis mokymasis, klasifikavimo algoritmai	tinklo pažeidimų aptikimas	tinklo saugumas	dinaminis	Atkūrimas
[95]	CNN	Skirtingi duomenų rinkiniai	biometrinis identifikavimas	statinis	Tikslumas
[69]	statistiniai metodai, mašininis mokymasis	UEBA	elgsenos analitika	statinis	EER
[6]	mašininis mokymasis	sintetinių duomenų rinkiniai	vidinės grėsmės aptikimas	N/A	F-score, TNR, FPR, AUC
[87]	mašininis mokymasis, atstumo funkcijos	CMU	klaviatūros dinamika	statinis	FAR, FPR, EER
[82]	gilusis mokymasis	GREYC-NISLAB	klaviatūros dinamika	statinis	EER
A.2	GAFMAT ir SNN	CMU, GREYC-NISLAB	klaviatūros dinamika	statinis	EER, Tikslumas

kad CNN galėtų efektyviai išgauti ir analizuoti šių vaizdų požymius. Tokia transformacija leidžia CNN išnaudoti visą savo matematinį potencialą, panaudojant galingas požymių išskyrimo galimybes, būdingas vaizdo duomenims [24, 35, 119]. Rekomenduojama klaviatūros laiko eilučių duomenis transformuoti į vaizdus, naudojant Gramiano kampinį sumos/skirtumo lauką (angl. *Gramian Angular Summation/Difference Field*, toliau GASF/GADF), Markovo perėjimų lauką (angl. *Markov Transition Field*, toliau MTF), pasikartojimo diagrama (angl. *Recurrence Plot*, toliau RP) ir panašias metodikas [24, 35]. SNN su CNN atšakomis ir laiko eilučių transformacija į vaizdus, gali tapti tvirtu patikimo naudotojo autentiškumo nustatymo pagrindu. Tai aktualu kibernetinėje aplinkoje, kur svarbu greitai nustatyti ir blokuoti neautorizuotus prisijungimus, kartu išlaikant patogią naudotojo sąveiką.

Skyriaus išvados

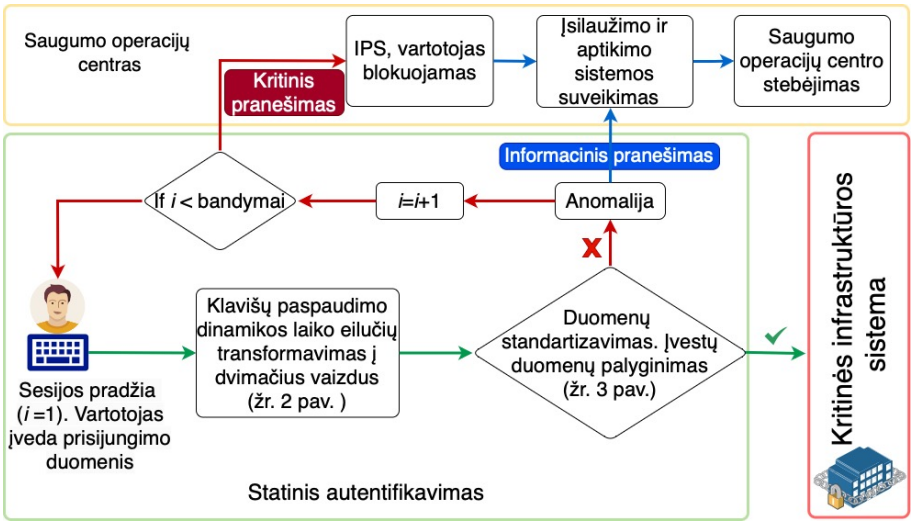
Apžvelgtoje literatūroje pabrėžiama, kad nors slaptažodžių sistemos vis dar plačiai naudojamos, jų trūkumai – tokie kaip silpni prisijungimo duomenys ir pažeidžiamumas atakoms – rodo aiškų poreikį patikimesniems sprendimams. Viena iš perspektyviausių alternatyvų yra elgsenos biometrija, klavišų paspaudimo dinamika, kuri leidžia patikrinti naudotojo tapatybę nenaudojant papildomos techninės įrangos. Giliojo mokymosi metodų, SNN ir CNN tinklų, naudojimas gerokai padidina autentiškumo nustatymo sistemos tikslumą ir patikimumą. Nepaisant šių privalumų, reikia dar labiau sumažinti EER ir užtikrinti, kad siūlomi metodai būtų praktiškai pritaikomi realioje aplinkoje. Ateities tyrimuose svarbu sutelkti dėmesį į duomenų kintamumo valdymą ir testavimą su įvairiais duomenų rinkiniais, siekiant efektyviau pritaikyti klaviatūros dinamiką kibernetiniam saugumui stiprinti.

S.2. NAUDOTOJO AUTENTIŠKUMO NUSTATYMO METODIKA

Siekiant apsaugoti ypatingos svarbos infrastruktūrą, labai svarbus veiksmingas naudotojų autentiškumo patvirtinimas. Šiame skyriuje pristatoma, kaip klavišų paspaudimų dinamiką galima integruoti į statinį prisijungimą ir nuolatinę sesijos stebėseną. Taip pat aptariamas neuroninių tinklų, tokių kaip SNN ir CNN panaudojimas, bei duomenų transforma-

cija į vaizdinius atvaizdus. Panašūs sprendimai leidžia aptikti vidines grėsmes, net jei neįgaliotas asmuo žino slaptažodį [11, 43].

Statinis autentifikavimas tikrina naudotojo unikalų spausdinimo stilių tuo metu, kai jis įveda slaptažodį. S.1 paveiksle parodytas klaviatūros sugeneruotų laiko žymų (angl. *timestamps*) transformacija į vaizdus ir jų palyginimo su atitinkama duomenų baze procesas. Jei nerandama atitikmenų, sistema įspėja apie galimą nesankcionuotą bandymą prisijungti.



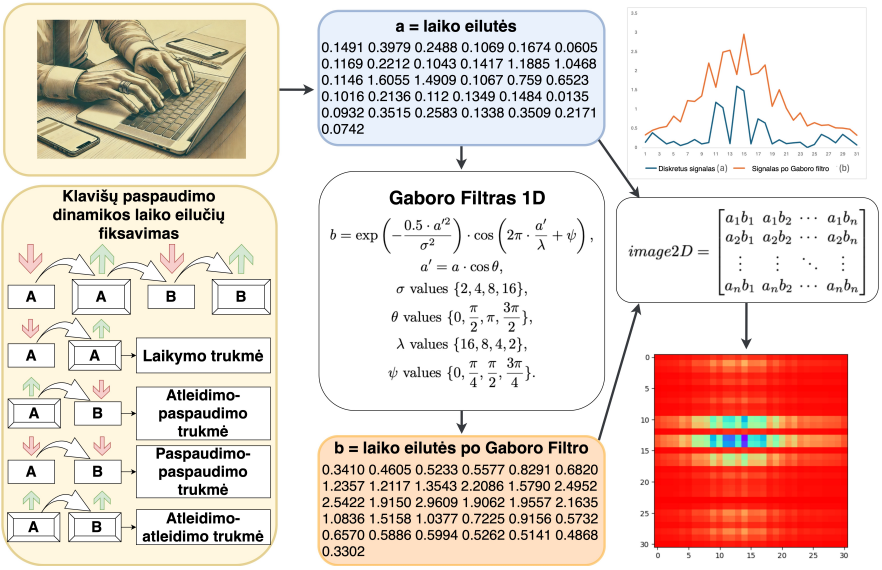
S.1 pav.: Įsilaužimo aptikimo ir prevencijos sistema, identifikuojanti naudotoją pagal dinaminius klaviatūros požymius.

Šis sprendimas suteikia galimybę integruoti slaptažodžių autentiškumo nustatymo metodus į ypatingos svarbos infrastruktūrą. Sudėtingiausia nustatyti klavišų paspaudimų dinamikos panašumą, norint nustatyti, ar slaptažodį įvedė teisėtas naudotojas, ar įsilaužėlis.

S.2.1. Duomenų transformacija į vaizdus

Taikant kai kurias programas, būtina skaitmeninius duomenis paversti vaizdais, kad CNN galėtų veiksmingai išgauti ir analizuoti šių vaizdų požymius. Tokia transformacija leidžia CNN išnaudoti visą jų matematinį potencialą, pasitelkiant požymių išskyrimo funkcijas, kurios iš esmės skirtos vaizdų duomenims [24, 35, 119]. Išdėstant požymius dvimatėje erdvėje, galima išryškinti jų tarpusavio ryšius, todėl CNN pagrįsti mode-

liai gali išskirti požymius, kurie dažnai pranoksta tradicinius metodus, besiremiančius tik skaitiniais įvesties duomenimis. Pasinaudodami šiais požymių ryšiais, CNN gali pagerinti prognozavimo ar klasifikavimo rezultatus, palyginti su modeliais, apmokytais skaitiniais duomenimis [119]. Remiantis įžvalgomis, gautomis analizuojant literatūrą ir nagrinėjant skaitinių duomenų transformacijos į vaizdus naudą, šio darbo autorius sukūrė naują skaitinių duomenų transformacijos į vaizdus metodą – GAFMAT (žr. S.2 paveikslą).



S.2 pav.: GAFMAT metodas, skirtas klavišų paspaudimo dinamikos laiko eilutėms transformuoti į dvimačius vaizdus. Viršutiniame kairiajame kampe esantis vaizdinis elementas pritaikytas iš [32].

Kai įvedamas slaptažodis, sukuriamas nuoseklus duomenų rinkinys, kuriame fiksuojamos kiekvieno klavišo paspaudimo dinamikos laiko žymos. Laiko žymos sudaromos iš klavišo laikymo trukmės, klavišų atleidimo ir paspaudimo trukmės, paspaudimo ir paspaudimo trukmės bei atleidimo ir atleidimo trukmės. Ši laiko seka sudaro diskrečią reikšmių seką a (parodyta S.2 paveikslo viršuje), kuri atspindi unikalų naudotojo rašymo ritmą ir greitį.

Sekantis žingsnis yra Gaboro filtro taikymas, kuris matematiškai aprašytas ir vizualiai pavaizduotas centrinėje S.2 paveikslo dalyje. Šis filtras pritaikomas taip, kad išryškintų klavišų paspaudimų dinamikos

savybes. Metodo esmė yra taikyti Gaboro filtrą diskrečiam signalui, kuris atspindi klavišų paspaudimų duomenis.

Gaboro filtrai, kurių parametrai yra filtro plotis (σ), orientacija (θ), bangos ilgis (λ) ir fazės poslinkis (ψ), parenkami iš reikšmių rinkinio, kad išryškintų svarbiausius duomenų požymius. Dėl šios priežasties a signalas paverčiamas b signalu. Gaboro filtro nustatymą sudaro operacijų seka, kai filtras kiekvieną kartą iš naujo taikomas su skirtingais unikalių parametrų rinkiniais. Po to, kai Gaboro filtras pritaikomas klavišų paspaudimų signalui ir iš pradinių duomenų a sukuriamas transformuotas signalas b, šie duomenys naudojami vaizdo formavimui. Transformuotas signalas kartu su pradine klavišų paspaudimų dinamika yra apdorojamas taikant išorinės sandaugos operaciją. Šios operacijos rezultatas yra dvimatis vaizdas, kuriame pradiniai laiko eilučių duomenys paverčiami vizualiai interpretuojamu formatu. Tai reiškia, kad klavišų paspaudimų laiko pokyčiai ir jų pasikartojantys modeliai yra išreiškiami kaip vizualūs elementai – spalvų ar intensyvumo pasiskirstymas vaizde.

S.2.2. Siamo neuroninių tinklų architektūros taikymas naudotojų autentifikavimui

1993 m. buvo pristatytas Siamo neuroninio tinklo pagrindu sukurtas parašų tikrinimo uždavinių sprendimo metodas [15]. Šis metodas apima dviejų įvesties pavyzdžių palyginimą, siekiant nustatyti jų panašumą. Tinklo architektūra buvo sukurta spręsti uždavinius, susijusius su poriniais palyginimais. Laikui bėgant SNN dėl savo gebėjimo efektyviai spręsti užduotis, sulaukė didelio populiarumo įvairiose srityse, įskaitant veido atpažinimą, vaizdų palyginimą ir biometrinį autentifikavimą.

Šioje disertacijoje SNN architektūra naudoja tris CNN atšakas ir trejetų nuostolių funkciją išvesties sluoksnyje [15, 89]. Tokia konfigūracija leidžia efektyviai įvertinti atstumą tarp vaizdų [21, 28, 29, 88, 111] (žr. S.3 paveikslą tinklo mokymo dalyje). Mokant SNN dažnai naudojami trejetai (angl. *triplets*), sudaryti iš inkaro, teigiamo ir neigiamo pavyzdžio:

- inkaras (angl. *Anchor*, toliau A) – elementas su kuriuo lyginami kiti elementai,
- teigiamas (angl. *Positive*, toliau P) elementas – panašus arba susijęs

su inkaru,

- neigiamas (angl. *Negative*, toliau N) elementas – nėra panašus ar susijęs su inkaru.

Po mokymo SNN sukuria atitinkamus visų trejetų įterpinius. Šie įterpiniai yra daugiamatės latentinės erdvės vektoriai, atspindintys įvesties duomenis arba šiuo atveju vaizdus. Pagrindinė idėja yra ta, kad panašūs vaizdai šioje erdvėje sukuria arti vienas kito esančius įterpinius, o nepanašūs vaizdai sukuria įterpinius, kurie yra labiau nutolę vienas nuo kito.

S.2.3. Duomenų vizualizavimas ir duomenų standartizavimo metodai

Naudotojo autentiškumo patvirtinimo klavišų paspaudimų dinamikos kontekste dažnai tenka susidurti su daugiamačiais duomenimis. Kiekvienas klavišo paspaudimo įvykis sukuria daugybę požymių, pavyzdžiui, klavišo paspaudimo trukmę, trukmę tarp klavišų paspaudimų ir rašymo ritmą. Šiems sudėtingiems duomenims analizuoti šiame darbe naudojama SNN su trejetų nuostolių funkcija. Šis tinklas apdoroja klavišų paspaudimų duomenis ir sukuria daugiamatį įterpinį. Tačiau šių įterpinių, paprastai esančių 256 ar daugiau matmenų erdvėje, negalima tiesiogiai interpretuoti. Dimensijų mažinimo ir duomenų vizualizavimo metodai yra svarbūs mašininio mokymosi srityje, analizuojant sudėtingus duomenis [14, 31, 53, 68, 77, 85, 118]. Vizualizavimas ne tik patvirtina tinklo gebėjimą atskirti naudotojus, bet ir suteikia intuityvų būdą įvertinti sistemos veikimą ir patikimumą.

Šie metodai vertingi atliekant tiriamąją analizę, nes suteikia galimybę įžvelgti panašumo ryšius daugiamatėje duomenų sistemoje. Neuroninių tinklų architektūrų derinimas su žinomais vizualizavimo metodais leidžia vizualiai atvaizduoti gautą informaciją ir pagerina interpretavimo galimybes.

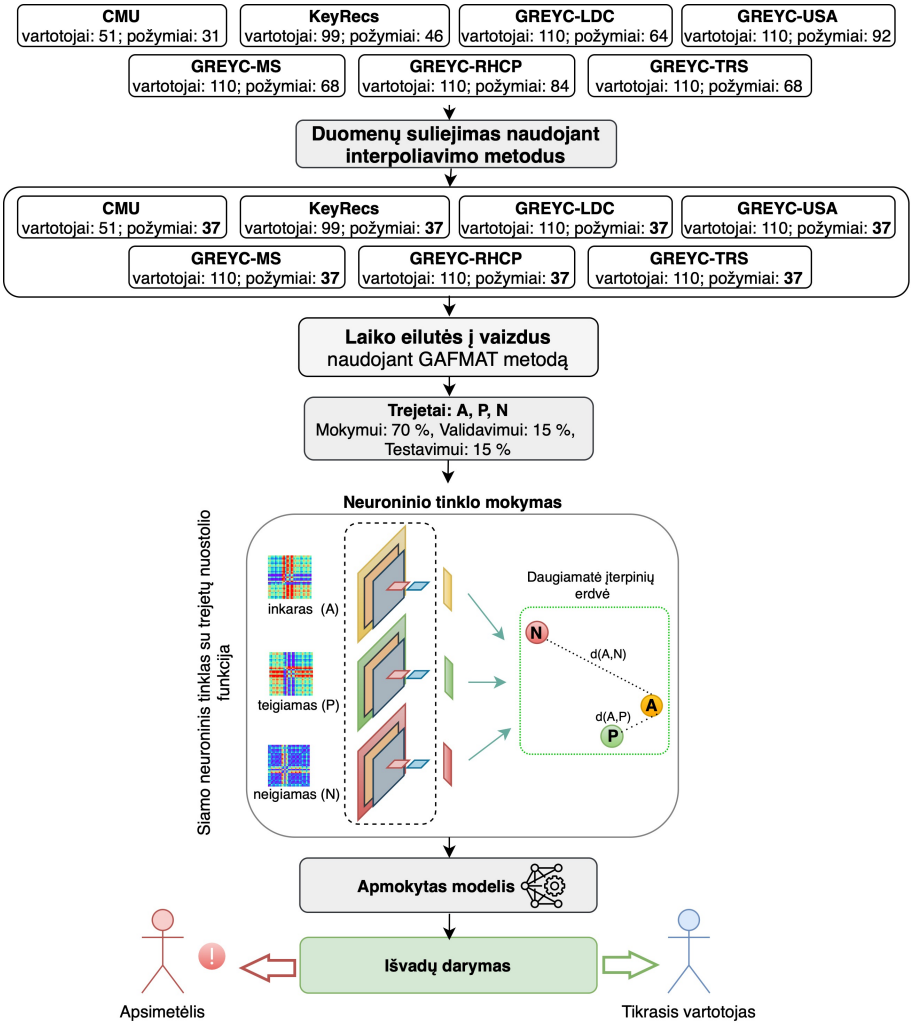
Vienas iš svarbių iššūkių slaptažodžiais grįstose autentifikavimo sistemose yra skirtingas slaptažodžių ilgis tarp naudotojų. Siekiant sukurti universalią metodiką, leidžiančią neuroninį tinklą pritaikyti prie įvairaus ilgio slaptažodžių, būtina iš anksto standartizuoti įvesties duomenų ilgį. Tai leidžia naudoti vieną apmokytą modelį, nereikalaujant kurti atskirų modelių kiekvienam naujam slaptažodžiui. SNN atveju, kai reikalingas pastovus įvesties dydis, laiko eilučių ilgio stan-

dartizavimas tampa itin svarbus. Šiai problemai spręsti taikomi įvairūs interpoliavimo metodai [60], kurie, nors ir sukurti trūkstamoms laiko eilučių reikšmėms atkurti, taip pat veiksmingai pritaikomi įvesties ilgiui suvienodinti [17]. Tokiu būdu užtikrinamas duomenų nuoseklumas ir galimybė tinklui tiksliai apdoroti skirtingo ilgio slaptažodžius.

S.3 paveiksle pateikta metodika skirta naudotojų autentiškumui nustatyti analizuojant unikalias klavišų paspaudimų dinamikos charakteristikas. Joje pateikiamas sistemingas visų slaptažodžių suvienodinimo metodas naudotojo tapatybei nustatyti. Iš pradžių CMU, KeyRecs ir GREYC-NISLAB duomenų rinkiniai, kurie skiriasi naudotojų ir požymių skaičiumi, prieš tolesnį apdorojimą standartizuojami interpoliuojant iki vienodo požymių skaičiaus, kad būtų užtikrintas vienodumas. CMU duomenų rinkinį [56] sudaro 51 dalyvis, iš kurių kiekvienas turėjo įvesti slaptažodį „.tie5Roanl“ 50 kartų per sesiją, atliekant aštuonis seansus. Požymių skaičius CMU yra 31. KeyRecs duomenų rinkinį [26] sudaro 99 dalyviai iš viso pasaulio, kurių kiekvienas įvesdavo „vpwjkeurkb“ slaptažodį, sudarydami iš viso 19 773 įvestis. Požymių skaičius KeyRecs yra 46. GREYC-NISLAB duomenų rinkinyje [41] yra penki skirtingi slaptažodžiai, kuriuos įvedė 110 naudotojų. Požymių skaičius varijuoja nuo 64 iki 92. Slaptažodžiai yra tokie: „leonardo dicaprio“, „the rolling stones“, „michael schumacher“, „red hot chilli peppers“ ir „united states of america“. Toliau tekste GREYC-NISLAB duomenų rinkinio slaptažodžiai vadinami LDC, TRS, MS, RHCP ir USA, atitinkantys kiekvieną konkretų slaptažodį. Taikant šią metodiką pavaizduotą S.3 paveiksle keli duomenų rinkiniai integruojami į standartizuotą formatą, kad būtų užtikrintas nuoseklus SNN mokymas. Išvados etape naudotojo slaptažodžio pavyzdys paverčiamas vaizdu ir apdorojamas apmokytu SNN, siekiant sukurti įterpinį. Jis lyginamas su ankstesniais įterpiniais, o atstumas tarp jų vertinamas pagal nustatytą ribą, grįstą istorinių prisijungimų duomenimis, siekiant nustatyti autentiškumą.

Skyriaus išvados

Aprašytas autentifikavimo metodas, pagrįstas klavišų paspaudimo dinamika, suteikia patikimą būdą apsaugoti kritinę infrastruktūrą. Naudojant SNN ir CNN tinklus bei GAFMAT transformacijos metodą, kuris klavišų paspaudimų duomenis transformuoja į vaizdus, sistema efek-



S.3 pav.: Duomenų suvienodinimu grindžiamo autentiškumo nustatymo sprendimas naudojant klavišų paspaudimų dinamikos analizę.

tyviai išgauna požymius ir prisitaiko prie įvairaus ilgio slaptažodžių. Duomenų vizualizavimo ir standartizavimo metodai užtikrina daugiamačių duomenų interpretavimą bei apdorojimą, suteikdami universalią ir lanksčią autentifikavimo sistemą, pritaikytą realioms sąlygoms.

S.3. EKSPERIMENTAI IR REZULTATAI

Prieš pradedant duomenų analizę, atsitiktine tvarka buvo atrinkti penki CMU duomenų rinkinio naudotojai, kurių duomenys (iš viso 2 000

pavyzdžių) buvo atskirti ir patalpinti į atskirą aplanką. Šis atskyrimas buvo atliktas siekiant užtikrinti, kad dirbtinio neuroninio tinklo mokymo metu šie duomenys nedarytų jokios įtakos modeliui. Likusių 46 individų duomenys, sudarantys 18 400 pavyzdžių, buvo naudojami tinklo mokymui. Tiek mokymo ir validavimo duomenys (18 400 pavyzdžių), tiek testavimo duomenys (2 000 pavyzdžių iš penkių naudotojų) buvo paversti vaizdais. Šiame etape buvo sukurti penki atskiri duomenų rinkiniai, kiekvienas skirtas tinklo mokymui ir testavimui, kuriuose tie patys duomenys buvo apdoroti taikant skirtingus transformacijos metodus: GASF, GADF, MTF, RP ir GAFMAT. Kas antras slaptažodžio pavyzdys buvo laikomas naudotojo slaptažodžio įvedimo elgsenos inkaru, o iškart po jo einantys bandymai – teigiamais pavyzdžiais. Toks skirstymas buvo pagrįstas pastebėjimu, kad su slaptažodžiu susipažinę naudotojai laikui bėgant pagerina rašymo greitį ir išvysto stabilesnį rašymo stilių. Todėl lyginant inkarinius pavyzdžius su teigiamais pavyzdžiais reikėtų lyginti tuos, kurie laikui bėgant ir išmokus slaptažodį, tarp bandymų nebūtų nutolę vienas nuo kito. Todėl kiekvieną duomenų rinkinį sudarė 9 200 teigiamų pavyzdžių (paveikslėlių) ir 9 200 inkarinių pavyzdžių (paveikslėlių). 70 % sukurtų trejetų buvo naudojami mokymui, o likusieji 30 % – validavimui. Be to, testavimo tikslais testavimo duomenų rinkiniams buvo išskirta 1 000 teigiamų vaizdų ir 1 000 inkaro vaizdų. Norint sukurti SNN mokymo trejetus, inkaro ir teigiami pavyzdžiai buvo paimti iš to paties naudotojo, o neigiamas pavyzdys buvo atsitiktinai parinktas iš kito naudotojo. Ši procedūra buvo pakartota kiekvienam duomenų rinkiniui naudojant skirtingus transformacijos metodus.

S.2 lentelėje pateikti skirtingų transformacijos metodų rezultatai validavimo duomenų rinkiniui.

Atliekant visapusišką vertinimą, naudojant GAFMAT ir kitus transformacijos metodus buvo gauti daug žadantys rezultatai pagal kelis rodiklius:

- EER, biometrinėse autentiškumo nustatymo sistemose dažniausiai naudojamas tikslumo rodiklis (žr. S.1 lentelę),
- Plotas po kreive (angl. *Area Under Curve*, toliau AUC),
- Euklidinis atstumas (angl. *Euclidean Distance*, toliau ED) tarp A ir P įterpinių daugiamatėje latentinėje erdvėje (angl. *Anchor-Positive Euclidean Distance*, toliau AP_ED),

S.2 lentelė: Vaizdų transformacijos metodų rezultatai, gauti CMU duomenų rinkiniui, naudojant GADF, GASF, RP, MTF ir GAFMAT metodus.

	Transformacijos į vaizdus metodai				
Metrikos	**GADF**	**GASF**	**RP**	**MTF**	**GAFMAT**
Accuracy↑	**0,99077**	0,98473	0,98331	0,94744	0,98935
EER↓	0,04794	0,05540	0,05327	0,12074	**0,04545**
AUC↑	0,98612	0,98290	0,98394	0,94862	**0,98668**
AP_ED↓	0,44127	0,47255	**0,43633**	0,56487	0,48600
AN_ED↑	1,72784	1,71689	1,68884	1,59469	**1,76378**
AP_STD↓	**0,27487**	0,29295	0,28245	0,36906	0,31383
AN_STD↓	0,32888	0,34455	0,34881	0,40005	**0,31295**
AN_CS↓	0,45772	0,45264	0,46871	0,46011	**0,43755**
AP_CS↑	**0,77936**	0,76373	0,78183	0,71756	0,75700

- ED tarp A ir N įterpinių daugiamatėje latentinėje erdvėje (angl. *Anchor-Negative Euclidean Distance*, toliau AN_ED),
- ED standartinis nuokrypis tarp A ir P įterpinių daugiamatėje latentinėje erdvėje (angl. *Anchor-Positive Standard Deviation*, toliau AP_STD),
- ED standartinis nuokrypis tarp A ir N įterpinių daugiamatėje latentinėje erdvėje (angl. *Anchor-Negative Standard Deviation*, toliau AN_STD),
- Kosinuso panašumas tarp A ir P įterpinių daugiamatėje latentinėje erdvėje (angl. *Anchor-Positive Cosine Similarity*, toliau AP_CS),
- Kosinuso panašumas tarp A ir N įterpinių daugiamatėje latentinėje erdvėje (angl. *Anchor-Negative Cosine Similarity*, toliau AN_CS),
- Tikslumas (angl. *Accuracy*).

Eksperimentų rezultatai parodė, kad taikant GAFMAT metodą pasiekiami stabilesni rezultatai, kuriems būdingi mažesni svyravimai nei naudojant kitus transformacijos metodus. Nors EER reikšmės statistiškai reikšmingai nesiskyrė, GAFMAT dažnai pasižymėjo šiek tiek geresniais rodikliais. Tai rodo šio metodo veiksmingumą transformuojant skaitinius duomenis į vaizdus. Pradiniuose eksperimentuose pastebėta,

kad vaizdais paversti klavišų paspaudimų duomenys užtikrino geresnius tinklo mokymo rezultatus, palyginti su neapdorotais duomenimis (žr. S.3 lentelę). Manoma, kad tokia transformacija pagerina duomenų interpretaciją ir naudotojo atpažinimą.

Svarbu pažymėti, kad testavimo duomenų rezultatai (žr. S.4 lentelę) buvo ženkliai prastesni nei validavimo. SNN dažnai klaidingai klasifikuodavo vieną iš penkių neigiamų pavyzdžių kaip teigiamą, kas rodo padidėjusį klaidingų teigiamų atvejų skaičių. Vis dėlto analizė atskleidžia, kad GAFMAT ir kiti transformacijos metodai išlieka perspektyvūs taikant juos testavimo rinkiniams.

S.3 lentelė: CMU rezultatų palyginimas.

Šaltiniai	**Metodai**	**EER**
Skyrius S.3	GAFMAT	**0,04545**
[56] (originalus)	Manheteno atstumas (normuotas)	0,09600
[116]	Artimiausio kaimyno (nauja atstumo metrika) + išskirčių šalinimas	0,08400
[116]	Artimiausio kaimyno (nauja atstumo metrika)	0,08700
[73]	Indukcinis perdavimo enkoderis (Manheteno atstumas)	0,06300
[18]	CNN	0,06500
[49]	Hierarchinis klasterizavimas naudojant Manheteno atstumą	0,07700
[87]	Manheteno atstumas (pagal standartinį nuokrypį)	0,09160

Analogiški eksperimentai atlikti su CMU duomenų rinkiniu buvo pakartoti su GREYC-NISLAB duomenų rinkiniu. Duomenys buvo suskirstyti pagal tą pačią struktūrą, kaip ir CMU atveju, tačiau šį kartą visi slaptažodžiai buvo konvertuoti naudojant tik GAFMAT metodą. Tolesnėse lentelėse pateikiami rezultatai, gauti įvertinus validavimo (žr. S.5 lentelę) ir testavimo (žr. S.6 lentelę) duomenis, siekiant įvertinti bendrą metodo efektyvumą ir palyginti jį su ankstesniais eksperimentais.

Rezultatai, gauti naudojant CMU duomenų rinkinį, rodo, kad skaitines vertes transformuojant į vaizdus tokiais metodais kaip GADF, GASF ir RP, EER reikšmės buvo atitinkamai 0,04794, 0,0554 ir 0,05327. Svarbu pažymėti, kad pasiūlytasis skaitinių duomenų transformacijos į vaizdus

S.4 lentelė: Vaizdų transformacijos metodų rezultatai, gauti naudojant CMU testavimo duomenų rinkinio klavišų paspaudimų dinamikos duomenis, naudojant GADF, GASF, RP, MTF ir GAFMAT.

	Transformacijos į vaizdus metodai				
Metrikos	**GADF**	**GASF**	**RP**	**MTF**	**GAFMAT**
Accuracy↑	**0,86800**	0,8540	0,82900	0,85400	0,86600
EER↓	**0,21000**	0,24500	0,23900	0,24500	0,21500
AUC↑	0,85928	0,83398	0,83937	0,83398	**0,85951**
AP_ED↓	**0,73164**	0,86555	0,84481	0,86555	0,83616
AN_ED↑	1,41323	1,50249	1,50904	1,50249	**1,52453**
AP_STD↓	**0,41727**	0,45697	0,47537	0,45697	0,44798
AN_STD↓	0,43871	0,44504	0,44953	0,44504	**0,42488**
AN_CS↓	0,46378	**0,40799**	0,41154	**0,40799**	0,40983
AP_CS↑	**0,63418**	0,56723	0,57760	0,56723	0,58192

S.5 lentelė: Rezultatai, gauti naudojant GREYC-NISLAB validavimo duomenų rinkiniams, kai klavišų paspaudimų dinamikos laiko eilučių požymiai transformuojami į vaizdą naudojant GAFMAT metodą.

	Slaptažodžiai (GREYC-NISLAB)				
Metrikos	**leonardo dicaprio**	**the rolling stones**	**michael schumacher**	**red hot chilli peppers**	**united states of america**
Accuracy↑	0,97656	0,98698	0,99219	0,97778	**0,99220**
EER↓	0,07552	0,04688	0,0651	**0,04444**	0,04688
AUC↑	0,97824	0,98667	0,98771	0,98272	**0,98847**
AP_ED↓	0,44736	0,43986	0,39958	0,45165	**0,39566**
AN_ED↑	1,55644	1,61202	1,48864	**1,63478**	1,61275
AP_STD↓	0,24318	0,21992	0,20467	0,21505	**0,19676**
AN_STD↓	0,40601	**0,37381**	0,38351	0,38917	0,38013
AN_CS↓	0,49905	0,48703	0,52795	**0,47839**	0,49790
AP_CS↑	0,77632	0,78007	0,80021	0,77417	**0,80217**

metodas GAFMAT pasiekė žemiausią EER 0,04545. Naudojant GREYC-NISLAB duomenų rinkinį, GAFMAT metodas pasiekė EER reikšmes, svyruojančias nuo 0,04444 iki 0,07552.

S.6 lentelė: Rezultatai, gauti naudojant GREYC-NISLAB testavimo duomenų rinkiniams, kai klavišų paspaudimų dinamikos laiko eilučių požymiai transformuojami į vaizdą naudojant GAFMAT metodą.

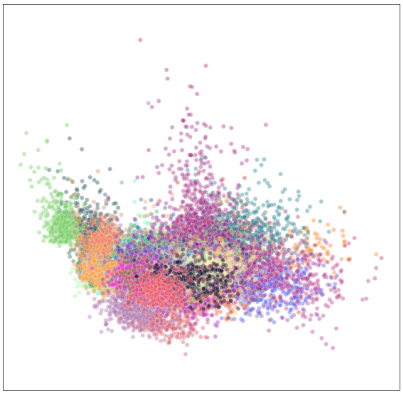
Metrikos	Slaptažodžiai (GREYC-NISLAB)				
	leonardo dicaprio	**the rolling stones**	**michael schumacher**	**red hot chilli peppers**	**united states of america**
Accuracy↑	0,84000	0,86000	0,86000	0,84000	**0,92000**
EER↓	0,16000	0,20000	0,22000	0,22000	**0,14000**
AUC↑	**0,90320**	0,85920	0,85400	0,86680	0,89240
AP_ED↓	0,78894	0,86642	**0,67407**	0,87670	0,75085
AN_ED↑	**1,55808**	1,49985	1,33055	1,55131	1,50073
AP_STD↓	0,41371	0,40861	**0,31141**	0,44201	0,43587
AN_STD↓	**0,40956**	0,41111	0,49554	0,40963	0,42794
AN_CS↓	0,41324	0,40843	0,49884	**0,39300**	0,43711
AP_CS↑	0,60553	0,56679	**0,66297**	0,56165	0,62458

S.3.1. Klavišų paspaudimų dinamikos duomenų vizualizavimo eksperimentai ir rezultatai

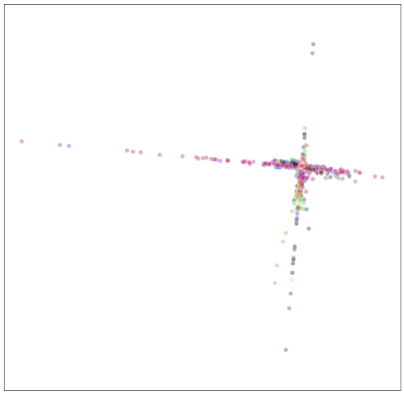
Šiame poskyryje demonstruojamos vizualizavimo sistemos, analizuojančios naudotojo klavišų paspaudimų dinamiką. S.4 paveiksle pateikiami rezultatai, gauti taikant įvairius dimensijos mažinimo metodus (PCA, LLE, UMAP ir t-SNE) neapdorotam CMU duomenų rinkiniui.

Pritaikius siūlomą naudotojo autentifikavimo metodiką, kurioje skaitiniai duomenys transformuojami į GAFMAT ir paduodami SNN su CNN atšakomis, buvo atvaizduoti kiekvieno įvesto CMU slaptažodžio įterpiniai (žr. S.5 paveikslą).

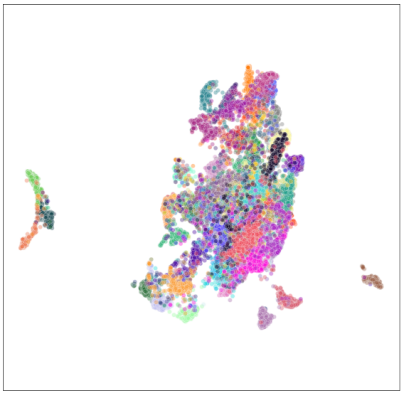
Vizualizavimo metodų dėka galima aiškiai pamatyti, kaip GAFMAT transformacija ir SNN pagrįstas autentiškumo nustatymo metodas leidžia efektyviau atskirti naudotojo duomenų įterpinius, palyginti su originaliais skaitiniais duomenimis. Dėl to galima aiškiau atskirti skirtingus naudotojus ir saugumo analitikai gali veiksmingiau aptikti potencialias anomalijas ir vidines grėsmes ypatingos svarbos infrastruktūros aplinkoje.



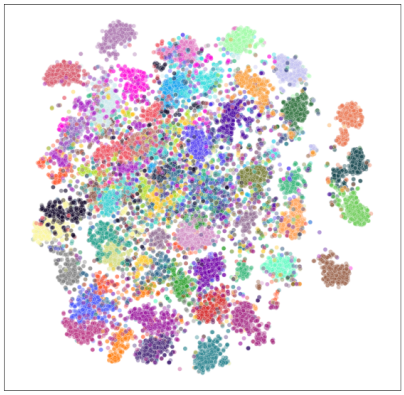
(a) PCA



(b) LLE



(c) UMAP



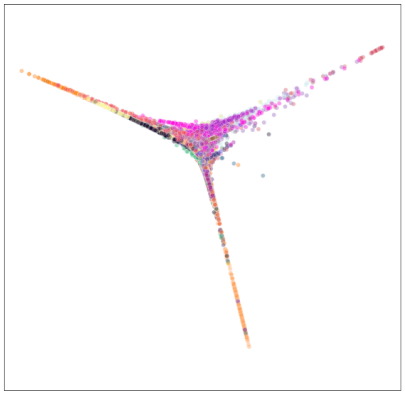
(d) t-SNE

S.4 pav.: Daugiamatės duomenų vizualizacijos naudojant skirtingus dimensijų mažinimo metodus: a) PCA, b) LLE, c) UMAP, d) t-SNE. Kiekviena spalva atitinka skirtingą CMU duomenų rinkinio naudotoją.

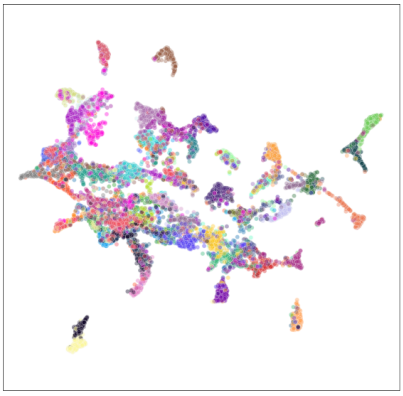
S.3.2. Klavišų paspaudimo dinamikos duomenų standartizavimu pagrįsti eksperimentai ir rezultatai

Šiame skyriuje išsamiai aprašoma eksperimentų serija, kuria siekiama pademonstruoti siūlomo duomenų standartizavimo metodo (žr. S.2.3 poskyrį) veiksmingumą tvarkant skirtingo ilgio klavišų paspaudimų dinamikos duomenis, pabrėžiant jo galimybes patobulinti naudotojo autentifikavimą. Aptariami klavišų dinamikos duomenų sujungimo eksperimentų rezultatai ir jų palyginimas su ankstesniais tyrimais. Tyrime buvo naudojama ANOVA analizė, siekiant nustatyti, ar skirtingų

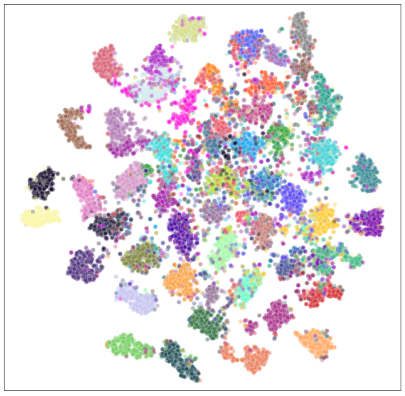
(a) PCA



(b) LLE



(c) UMAP



(d) t-SNE

S.5 pav.: Daugiamačių įterpinių, gautų naudojant SNN, vizualizavimas taikant skirtingus dimensijos mažinimo metodus ($p = 256$): (a) PCA, (b) LLE, (c) UMAP, (d) t-SNE. Kiekviena spalva atitinka skirtingą CMU duomenų rinkinio naudotoją.

interpoliacijos metodų taikymas turi statistiškai reikšmingą poveikį EER. Rezultatai rodo, kad interpoliacijos metodų skirtumai nėra statistiškai reikšmingi, nes p-reikšmės viršijo 0,05 slenkstį. Tai reiškia, kad pastebėti skirtumai gali būti paaiškinami atsitiktiniais svyravimais, o ne realiais metodų efektyvumo skirtumais.

Naudojant CMU duomenų rinkinį nustatyta, kad tiesinė interpoliacija buvo efektyviausia, kuri užtikrino mažiausią EER, aukščiausią tikslumą ir rezultatų pastovumą. Priešingai, kubinė ir artimiausio kaimyno interpoliacijos metodai pasižymėjo didesniais rezultatų svyravimais.

Atlikti panašūs eksperimentai su KeyRecs duomenų rinkiniu, kuriam būdingas didesnis požymių skaičius. Rezultatai parodė, kad artimiausio kaimyno interpoliacija pasižymėjo šiek tiek mažesniu vidutiniu EER nei bitiesinė (angl. *bilinear*) ar kubinė interpoliacija. Nors bitiesinis metodas kai kuriais atvejais užtikrino didesnį tikslumą, jo stabilumas buvo mažesnis, palyginti su tiesine interpoliacija.

Pirmieji eksperimentai parodė, kad tiesinė interpoliacija yra tinkamiausias metodas klavišų paspaudimų duomenims standartizuoti. Atsižvelgus į šiuos rezultatus, GREYC-NISLAB duomenų rinkinio standartizavimui taip pat pasirinkta tiesinė interpoliacija. Šiame eksperimente slaptažodžiai buvo konvertuojami į fiksuoto ilgio 37 požymius, siekiant standartizuoti duomenis ir sukurti bendrą modelį tinkamą skirtingo ilgio slaptažodžiams. Analizė parodė, kad net ir esant skirtingiems slaptažodžių ilgiams, jų standartizavimas į vieną ilgį ir tiesinės interpoliacijos metodo taikymas padėjo pasiekti žemus EER rodiklius. Atlikti papildomi eksperimentai, sujungiant skirtingus klavišų paspaudimų dinamikos duomenų rinkinius į vieną, sistemos efektyvumui įvertinti. Buvo siekiama nustatyti, ar vienas modelis gali tiksliai atpažinti naudotojus, nepaisant jų naudojamų slaptažodžių ilgio. Eksperimentų rezultatai parodė, kad didžiausias tikslumas pasiektas tada, kai iš duomenų buvo pašalinti itin ilgi slaptažodžiai, nes jie dažnai lėmė didesnę klaidų variaciją.

S.3.3. Skyriaus išvados

Eksperimentų rezultatai parodė, kad GAFMAT metodas veiksmingai transformuoja klavišų paspaudimų dinamikos duomenis į vaizdus, leidžiančius taikyti giliuosius neuroninius tinklus naudotojų autentifikavimui. Tiesinė interpoliacija pasirodė tinkamiausia skirtingo ilgio slaptažodžiams standartizuoti, užtikrindama mažesnį EER ir modelio stabilumą. Fiksuoto ilgio požymių standartizavimas leidžia kurti universalią autentifikavimo sistemą, pritaikomą įvairiems duomenų rinkiniams. Be to, duomenų vizualizavimas padeda geriau interpretuoti modelio veikimą ir analizuoti naudotojų elgsenos ypatumus. Siūloma metodika pranoksta tradicinius sprendimus ir gali būti lengvai pritaikyta įvairiose autentifikavimo sistemose, neprarandant tikslumo ir stabilumo.

Šioje disertacijoje siūloma ir validuojama giliuoju mokymusi pagrįsta naudotojo autentifikavimo metodika, naudojanti klavišų paspaudimų dinamiką, skirta vidinių grėsmių aptikimui ypatingos svarbos infrastruktūroje. Pasiūlytoje metodikoje integruojami duomenų transformavimo iš nevaizdinių į vaizdinius metodai, duomenų suliejimo strategijos bei dimensijų mažinimo technikos, siekiant pagerinti modelio tikslumą, interpretavimą ir praktinį pritaikomumą.

Pagrindinės šio darbo išvados ir rezultatai:

- Pasiūlyta naudotojų autentifikavimo metodika, pagrįsta klaviatūros dinamika ir integruota SNN architektūra su CNN atšakomis, veiksmingai atskiria teisėtus naudotojus nuo neautorizuotos prieigos. Metodikos efektyvumas buvo patvirtintas taikant ją viešai prieinamiems duomenų rinkiniams.

- Transformuojant klaviatūros dinamikos duomenis į vaizdus naudojant GAFMAT, pagerino požymių išskyrimą ir modelio tikslumą, lyginant su kitais esamais metodais. CMU duomenų rinkinyje metodas pasiekė 0,04545 EER reikšmę. GREYC-NISLAB duomenų rinkinyje EER svyravo nuo 0,04444 iki 0,07552. Šie rezultatai rodo, kad GAFMAT efektyviai išryškina naudotojų rašymo elgseną ir padeda juos atskirti pagal rašymo stilių.

- Interpoliacija pagrįstomis duomenų suliejimo strategijomis, naudojant SNN architektūrą su CNN atšakomis, testavimo duomenyse iš sujungtų duomenų rinkinių buvo pasiekta 0,13281 EER reikšmė.

- SNN įterpinių vertinimui taikyti dimensijų mažinimo metodai parodė, kad šie įterpiniai reikšmingai pagerina naudotojų klasterių atskirtinumą, lyginant su neapdorotais duomenimis, silueto koeficientas padidėjo nuo 0,23 iki 0,52. Tai patvirtina, kad SNN efektyviai fiksuoja išskirtinius rašymo bruožus ir pagerina naudotojų atskyrimą autentifikavimo tikslais.

Notes

Arnoldas Budžys
Deep Learning-Based Keystroke Dynamics Authentication for Insider Threat Detection in Critical Infrastructure
Doctoral Dissertation
Natural Sciences
Informatics (N 009)
Thesis Editor: Rasa Raudienė

Arnoldas Budžys
Giliuoju mokymusi pagrįstas klavišų paspaudimų dinamikos autentifikavimas vidinių grėsmių aptikimui ypatingos svarbos infrastruktūroje
Daktaro disertacija
Gamtos mokslai
Informatika (N 009)
Santraukos redaktorė: Sigita Skukauskienė

Vilnius University Press
9 Saulėtekio Ave., Building III, LT-10222 Vilnius
Email: info@leidykla.vu.lt, www.leidykla.vu.lt
bookshop.vu.lt, journals.vu.lt
Print run of 20 copies