LITHUANIAN COMPUTER SOCIETY

VILNIUS UNIVERSITY INSTITUTE OF DATA SCIENCE AND DIGITAL TECHNOLOGIES

LITHUANIAN ACADEMY OF SCIENCES

DAMSS
DATA ANALYSIS METHODS FOR SOFTWARE SYSTEMS

14th Conference on

DATA ANALYSIS METHODS for Software Systems

November 30 – December 2, 2023

Druskininkai, Lithuania, Hotel "Europa Royale"
https://www.mii.lt/DAMSS

VILNIUS UNIVERSITY PRESS
Vilnius, 2023

Co-Chairmen:

Prof. Gintautas Dzemyda (Vilnius University, Lithuanian Academy of Sciences)
Dr. Saulius Maskeliūnas (Lithuanian Computer Society)

Programme Committee:

Dr. Jolita Bernatavičienė (Lithuania)
Prof. Juris Borzovs (Latvia)
Prof. Robertas Damaševičius (Lithuania)
Prof. Janis Grundspenkis (Latvia)
Prof. Janusz Kacprzyk (Poland)
Prof. Ignacy Kaliszewski (Poland)
Prof. Bożena Kostek (Poland)
Prof. Tomas Krilavičius (Lithuania)
Prof. Olga Kurasova (Lithuania)
Assoc. Prof. Tatiana Tchemisova (Portugal)
Prof. Julius Žilinskas (Lithuania)

Organizing Committee:

Dr. Jolita Bernatavičienė
Prof. Olga Kurasova
Assoc. Prof. Viktor Medvedev
Laima Paliulionienė
Assoc. Prof. Martynas Sabaliauskas
Prof. Povilas Treigys

Contacts:

Dr. Jolita Bernatavičienė
jolita.bernataviciene@mif.vu.lt
Prof. Olga Kurasova
olga.kurasova@mif.vu.lt
Tel. +370 5 2109315

Copyright © 2023 Authors. Published by Vilnius University Press.
This is an Open Access article distributed under the terms of the Creative Commons Attribution Licence, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

https://doi.org/10.15388/DAMSS.14.2023
ISBN 978-609-07-0985-6 (digital PDF)

© Vilnius University, 2023

Insider Threat Detection: A New Keystroke Dynamics-Based Approach to User Authentication in Critical Infrastructure

Arnoldas Budžys, Olga Kurasova, Viktor Medvedev

Institute of Data Science and Digital Technologies
Vilnius University

arnoldas.budzys@mif.stud.vu.lt

In today's evolving digital landscape, challenges such as unauthorised intrusions, cyber security breaches, and data compromise are threatening national defence, critical infrastructure, and economic sustainability. Robust authentication mechanisms are essential to address these vulnerabilities. Researchers are exploring the challenging problem of protecting critical infrastructure from insider threats, especially in the context of their increased levels of access and trust. To address this challenging problem, we present a deep learning-based methodology for user authentication. Our methodology is based on transforming keystroke time series data generated from passwords (numerical data) into images to increase the efficiency of intrusion detection and the accuracy of user verification. We present the GAFMAT (GAbor Filter MAtrix Transformation) method, a new approach for transforming numerical password data into a visual format. The Siamese neural network architecture with triplet loss function (or triplet network) is used to detect abnormal or unauthorised login entries. The authentication process based on this architecture compares the features of the password entered by the user and, using the proposed method, transformed into an image with previously known and transformed records, evaluating the authenticity against the reference transformed passwords stored in the database. We have proven the effectiveness of the GAFMAT method by using publicly available datasets and transforming them into visual representations. The experiments resulted in competitive and, in many cases, better EER (equal error rate) values compared to existing machine learning techniques. The robustness of GAFMAT to a range of passwords of different lengths and complexity confirms its potential as a reliable method for biometric authentication based on keystroke dynamics.