Lecture Notes on Data Engineering
and Communications Technologies 109

Sanjay Misra
Chamundeswari Arumugam *Editors*

Illumination of Artificial Intelligence in Cybersecurity and Forensics

Springer

Lecture Notes on Data Engineering and Communications Technologies

Volume 109

The aim of the book series is to present cutting edge engineering approaches to data technologies and communications. It will publish latest advances on the engineering task of building and deploying distributed, scalable and reliable data infrastructures and communication systems.

The series will have a prominent applied focus on data technologies and communications with aim to promote the bridging from fundamental research on data science and networking to data engineering and communications that lead to industry products, business knowledge and standardisation.

Indexed by SCOPUS, INSPEC, EI Compendex.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at https://link.springer.com/bookseries/15362

Sanjay Misra · Chamundeswari Arumugam
Editors

Illumination of Artificial Intelligence in Cybersecurity and Forensics

Springer

Editors
Sanjay Misra
Østfold University College
Halden, Norway

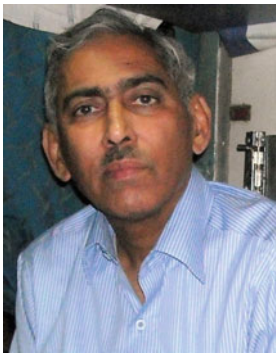
Chamundeswari Arumugam
Computer Science and Engineering
Sri Sivasubramaniya Nadar College
of Engineering
Chennai, Tamil Nadu, India

ISSN 2367-4512 ISSN 2367-4520 (electronic)
Lecture Notes on Data Engineering and Communications Technologies
ISBN 978-3-030-93452-1 ISBN 978-3-030-93453-8 (eBook)
https://doi.org/10.1007/978-3-030-93453-8

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

This Book is Dedicated to Father of Lead Editor Prof. Sanjay Misra

Mr. Om Prakash Misra



27.09.1950–24.12.2019

Preface

A new dimension in terms of illumination of AI is taken up here to showcase the relationship between AI and cybersecurity. This book supplies the related information that are concern in today's scenario in the field of cybersecurity and forensics. It takes you to the current techniques that are practically possible to apply in this domain using machine learning and deep learning concepts. The topic of cybersecurity in terms of IDS, authentication, audit techniques, forensics, IoT, health care, and image recognition are covered under various chapters. The research finding can be used as a base to improve the research thirst in this domain. Many empirical finding is available to explore the applicability of artificial intelligence in this domain. Also, the survey papers indicate many depth information on the applicability of artificial intelligence in this domain.

A pleasure to introduce the book, Illumination of AI in cybersecurity and forensics. Fifteen chapters organized in this book provide an interesting aspect of AI in cyber forensics and forensics. Some of chapters cover the applicability of preprocessing, feature selection, classification, analysis, prediction, dimensionality reduction, optimization, and AI techniques in this domain. The chapters demonstrate and report the dataset applicability in this domain using AI. The various datasets explored to provide the result outcomes are CIC-IDS2017, UNSW-NB15, KDD Cup 99, DARPA, etc. A brief summary of various authors presented in chapters is listed below.

Julián Gómez et al. in their chapter titled, "A Practical Experience Applying Security Audit Techniques in An Industrial Healthcare System", performed a security assessment process. The results of this study include a security audit on an industrial scenario currently in production. An exploitation and vulnerability analysis have been performed, and more that 450 vulnerabilities have been found. This chapter outlines a systematic approach using artificial intelligence to enable the system security team to facilitate the process of conducting a security audit taking into account the sensitivity of their systems.

Joseph Bamidele Awotunde et al., in their work titled "Feature Extraction and Artificial Intelligence-Based Intrusion Detection Model for a Secure Internet of Things Networks", discussed the security issues within IoT-based environments and the application of AI models for security and privacy in IoT-based for a secure network.

The chapter proposes a hybrid AI model framework for intrusion detection in an IoT-based environment and a case study using CIC-IDS2017 and UNSW-NB15 to test the proposed model's performance. The model performed better with an accuracy of 99.45%, with a detection rate of 99.75%. The results from the proposed model show that the classifier performs far better when compared with existing work using the same datasets, thus prove more effective in the classification of intruders and attackers on IoT-based systems.

Chika Yinka-Banjo et al. in their chapter titled, "Intrusion Detection Using Anomaly Detection Algorithm and Snort", focused on Intrusion Detection System (IDS) for a local network to detect network. A statistical approach, as well as a binomial classification, was used for simplicity in classification. The result shows the outlier value for each item considered; a 1 depicts an attack, a 0 depicts normalcy. The results are promising in dictating intrusion and anomalies in an IDS system.

Kousik Barik et al. in their chapter titled, "Research Perspective on Digital Forensic Tools and Investigation Process", provided a comparative analysis of popular tools in each category is tabulated to understand better, making it easy for the user to choose according to their needs. Furthermore, this chapter presents how machine learning, deep learning, and natural language processing, a subset of artificial intelligence, can be effectively used in digital forensic investigation. Finally, the future direction of the challenges and study scope in digital forensics and artificial intelligence is also mentioned for potential researches.

Timibloudi Stephen Enamamu in his chapter titled, "Intelligent Authentication Framework for Internet of Medical Things (IoMT)", explored the use of artificial intelligence to enhance authentication of Internet of Medical Things (IoMT) through a design of a framework. The framework is designed using wearable and or with a mobile device for extracting bioelectrical signals and context awareness data. The framework uses bioelectrical signals for authentication, while artificial intelligent is applied using the contextual data to enhance the patient data integrity. The framework applied different security levels to balance between usability and security on the bases of False Acceptance Rate (FAR) and False Rejection Rate (FRR). Thirty people are used for the evaluation of the different security levels and the security level 1 achieved a result base on usability verse security obtaining FAR of 5.6% and FRR of 9% but when the FAR is at 0%, the FRR stood at 29%. The Intelligent Authentication Framework for Internet of Medical Things (IoMT) will be of advantage in increasing the trust of data extracted for the purpose of user authentication by reducing the FRR percentage.

Stephen Bassi Joseph et al., in their chapter, "Parallel Faces Recognition Attendance System with Anti-Spoofing Using Convolutional Neural Network", proposed a parallel face recognition attendance system based on Convolutional Neural Network a branch of artificial intelligence and OpenCV. Experimental results proved the effectiveness of the proposed technique having shown good performance with recognition accuracy of about 98%, precision of 96%, and a recall of 0.96. This demonstrates that the proposed method is a promising facial recognition technology.

Kenneth Mary Ogbuka et al. in their chapter titled, "A Systematic Literature Review on Face Morphing Attack Detection (MAD)", explored to find MAD methodologies, feature extraction techniques, and performance assessment metrics that can help MAD systems become more robust. To fulfill this study's goal, a Systematic Literature Review was done. A manual search of 9 well-known databases yielded 2089 papers. Based on the study topic, 33 primary studies were eventually considered. A novel taxonomy of the strategies utilized in MAD for feature extraction is one of the research's contributions. The study also discovered that (1) single and differential image-based approaches are the commonly used approaches for MAD; (2) texture and key point feature extraction methods are more widely used than other feature extraction techniques; and (3) Bona-fide Presentation Classification Error Rate and Attack Presentation Classification Error Rate are the commonly used performance metrics for evaluating MAD systems. This chapter addresses open issues and includes additional pertinent information on MAD, making it a valuable resource for researchers developing and evaluating MAD systems.

Kenneth Mary Ogbuka et al., in their chapter titled, "Averaging Dimensionality Reduction and Feature Level Fusion for Post-Processed Morphed Face Image Attack Detection", proposed a MAD technique to perform MAD even after image sharpening operation using averaging dimensionality reduction and feature level fusion of Histogram of Oriented Gradient (HOG) 8 x 8 and 16 x 16 cell size. The 8 x 8 pixels cell size was used to capture small-scale spatial information from the images, while 16 x 16 pixels cell size was used to capture large-scale spatial details from the pictures. The proposed technique achieved a better accuracy of 95.71% compared with the previous work, which reached an accuracy of 85% when used for MAD on sharpened image sources. This result showed that the proposed technique is effective for MAD on sharpened post-processed images.

N. S. Gowri Ganesh et al. in their chapter, "A Systematic Literature Review on Forensics in Cloud, IoT, AI & Blockchain", reviewed the application of forensics using Artificial Intelligence in the field of Cloud computing, IoT, and Blockchain Technology. To fulfill the study's goal, a systematic literature review (SLR) was done. By manually searching six well-known databases, documents were extracted. Based on the study topic, 33 primary studies were eventually considered. The study also discovered that (1) highlights several well-known challenges and open issues in IoT forensics research, as it is dependent on other technologies and is crucial when considering an end-to-end IoT application as an integrated environment with cloud and other technologies. (2) There has been less research dedicated to the use of AI in the field of forensics. (3) Contributions on forensic analysis of attacks in blockchain-based systems is not found.

Mathew Emeka Nwanga et al. in their chapter titled, "Predictive Forensic Based—Characterization of Hidden Elements in Criminal Networks Using Baum-Welch Optimization Technique", contribute to knowledge by providing a terrorist computational model which helps to determine the most probable state and timeframe for the occurrence of terrorist attacks. It also provides the most probable sequence of active internal communications (AICs) that led to such attacks. The Baum–Welch optimization is applied in this research to improve the intelligence and

predictive accuracy of the activities of criminal elements. This solution is adaptable to any country around the globe. The result shows that the Foot Soldiers (FS) are most vulnerable with 90% involvement in criminal attacks; the Commander carried out most strategic (high profile) attacks estimated at 2.2%. The private citizens and properties had the highest attack targets (50.6%), whereas the police and military base had 12.3% and 6.7%, respectively. The results show that Boko-Haram carried out the greatest level of attacks at 79.2%, while Fulani extremists are responsible for 20.8% of all acts of terrorism in Nigeria from 2010 to date.

Roseline Oluwaseun Ogundokun et al. presented a chapter tiled, "An Integrated IDS Using ICA-Based Feature Selection and SVM Classification Method". Here, the authors presented a novel method for detecting security violations in IDSs that combines ICA FS and ML classifiers in this work. SVM was employed as a suitability function to identify important characteristics that can aid in properly classifying assaults. The suggested approach is utilized in this context to advance the resulting quality by changing the SVM regulatory parameter values. The goal was to achieve satisfactory results for the IDS datasets, KDD Cup 99, in terms of classifier performance in noticing invasions built on the optimal number of features. In contrast to several state-of-the-art approaches, the suggested model outperforms them in terms of accuracy, sensitivity, detection rate (DR) false alarm, and specificity. IDS may be used to secure wireless payment systems. It is possible to establish secure integrated network management that is error-free, therefore boosting performance.

Yakub Kayode Saheed, in his chapter titled, "A Binary Firefly Algorithm Based Feature Selection Method on High Dimensional Intrusion Detection Data", proposed a binary firefly algorithm (BFFA)-based feature selection for IDS. First performed normalization, subsequently, the BFFA algorithm was used for feature selection stage. Then adopted random forest algorithm for the classification phase. The experiment was performed on high-dimensional University of New South Wales-NB 2015 (UNSW-NB15) dataset with 75% of the data used for training the model and 20% for testing. The findings showed an accuracy of 99.72%, detection rate of 99.84%, precision of 99.27%, recall of 99.84%, and F-score of 99.56%. The results were gauge with the state-of-the-art results and our results were found outstanding.

Suleman Isah Atsu Sani et al. in their chapter titled, "Graphical Based Authentication Method Combined with City Block Distance for Electronic Payment System", proposed a graphical-based authentication method combined with an Artificial Intelligence (AI) domain city block distance algorithm to measure the similarity score between the image passwords at the points of registration and login. To achieve optimal performance of the system and make it robust, an experiment was conducted during the login session using the AI-based city block distance algorithm and other different distance algorithms that include Euclidean, Cosine similarity, and Jaccard. The experimental results show that the proposed city block distance method has the fastest execution time of 0.0318 ms, minimal matching error of 1.55231, and an acceptable login success rate of 64%, compared to when the graphical-based password is combined with other similarity score algorithms. This chapter concludes that the proposed method would be the most reliable authentication for e-payment systems.

S. Hanis et al. in their chapter titled, "Authenticated Encryption to Prevent Cyber-Attacks in Images", provided a secure authenticated encryption algorithm for the storage and transmission of digital images to avoid cyber threats and attacks. The designed algorithm makes use of the deep convolutional generative adversarial network to test if the image is a fake image originated by the intruder. If found fake exclusive OR operations are performed with the random matrices to confuse the intruder. If the image is not fake, then encryption operations are directly performed on the image. The image is split into two 4-bit images and a permutation operation using a logistic map is performed and finally the split images are merged together. Finally, exclusive OR operations are performed on the merged image using the convolution-based round keys generated to generate the concealed image. In addition, authentication is also achieved by calculating the mean of the actual image. The performance analysis shows that the designed technique offers excellent security and also helps in testing the authenticity of the stored images.

Vani Thangapandian in her paper titled, "Machine Learning in Automated Detection of Ransomware: Scope, Benefits and Challenges", proposed a Systematic Literature Review, to discuss the different ransomware detection tools developed so far and highlighted the strengths and weaknesses of Machine Learning-based detection tools. The main focus of this study is on how ransomware attacks are executed and the possible solutions to mitigate such attacks. The main focus of this work is the application of various machine learning and deep learning methods in detecting Ransomware. Many detection models that are developed with high accuracy have been discussed. Out of them, most of the models employ Machine Learning techniques for detection of ransomware as it facilitates automated detection. The proportion of the count (37.5%) of Machine Learning-based models is considerably higher than that of other models (3% each). The vital role of Machine Learning in developing automated detection tool is reviewed from different perspectives and the limitations of Machine Language-based model are also discussed.

This book discusses the AI in cybersecurity on various artifacts related to malware, image authentication, IoT, network, IoMT, facial recognition, criminal network, electronic payment system, etc. Hope this book serve the community who aspire to utilize the AI in cybersecurity and cyber forensics.

Halden, Norway/Ota, Nigeria — Sanjay Misra
Tamil Nadu, India — Chamundeswari Arumugam

Contents

A Practical Experience Applying Security Audit Techniques in An Industrial Healthcare System 1
Julián Gómez, Miguel Á Olivero, J. A. García-García, and María J. Escalona

Feature Extraction and Artificial Intelligence-Based Intrusion Detection Model for a Secure Internet of Things Networks 21
Joseph Bamidele Awotunde and Sanjay Misra

Intrusion Detection Using Anomaly Detection Algorithm and Snort 45
Chika Yinka-Banjo, Pwamoreno Alli, Sanjay Misra, Jonathan Oluranti, and Ravin Ahuja

Research Perspective on Digital Forensic Tools and Investigation Process 71
Kousik Barik, A. Abirami, Karabi Konar, and Saptarshi Das

Intelligent Authentication Framework for Internet of Medical Things (IoMT) 97
Timibloudi Stephen Enamamu

Parallel Faces Recognition Attendance System with Anti-Spoofing Using Convolutional Neural Network 123
Stephen Bassi Joseph, Emmanuel Gbenga Dada, Sanjay Misra, and Samuel Ajoka

A Systematic Literature Review on Face Morphing Attack Detection (MAD) 139
Mary Ogbuka Kenneth, Bashir Adebayo Sulaimon, Shafii Muhammad Abdulhamid, and Laud Charles Ochei

Averaging Dimensionality Reduction and Feature Level Fusion for Post-Processed Morphed Face Image Attack Detection 173
Mary Ogbuka Kenneth and Bashir Adebayo Sulaimon

A Systematic Literature Review on Forensics in Cloud, IoT, AI & Blockchain 197
N. S. Gowri Ganesh, N. G. Mukunth Venkatesh, and D. Venkata Vara Prasad

Predictive Forensic Based—Characterization of Hidden Elements in Criminal Networks Using Baum-Welch Optimization Technique 231
Mathew Emeka Nwanga, Kennedy Chinedu Okafor, Ifeyinwa Eucharia Achumba, and Gloria A. Chukwudebe

An Integrated IDS Using ICA-Based Feature Selection and SVM Classification Method 255
Roseline Oluwaseun Ogundokun, Sanjay Misra, Amos O. Bajeh, Ufuoma Odomero Okoro, and Ravin Ahuja

A Binary Firefly Algorithm Based Feature Selection Method on High Dimensional Intrusion Detection Data 273
Yakub Kayode Saheed

Graphical Based Authentication Method Combined with City Block Distance for Electronic Payment System 289
Suleman Isah Atsu Sani, John Kolo Alhassan, and Abubakar Saddiq Mohammed

Authenticated Encryption to Prevent Cyber-Attacks in Images 325
S. Hanis, N. Edna Elizabeth, R. Kishore, and Ala Khalifeh

Machine Learning in Automated Detection of Ransomware: Scope, Benefits and Challenges 345
Vani Thangapandian

About the Editors

Sanjay Misra is a Professor in Østfold University College, Halden Norway. Before Joining to Østfold University, he was full professor of Computer (software Engineering at Covenant University (400–500 ranked by THE(2019)) Nigeria for more than 9 yrs. He is PhD. in Inf. & Know. Engg (Software Engg) from the Uni of Alcala, Spain & M.Tech. (Software Engg) from MLN National Institute of Tech, India. As of today (21.05.2021)—as per SciVal(SCOPUS- Elsevier) analysis)—he is the most productive researcher (Number 1) https://t.co/fBYnVxbmiL in Nigeria during 2012–17,13–18,14–19 & 15–20 **(in all disciplines)**, in comp science no 1 in the country & no 2 in the whole continent. Total around 500 articles (SCOPUS/WoS) with 500 coauthors worldwide (-110 JCR/SCIE) in the core & appl. area of Soft Engg, Web engg, Health Informatics, Cybersecurity, Intelligent systems, AI, etc. He got several awards for outstanding publications (2014 IET Software Premium Award (UK)), and from TUBITAK (Turkish Higher Education and Atilim University). He has delivered more than 100 keynote/invited talks/public lectures in reputed conferences and institutes (traveled to more than 60 countries). He edited (with colleagues) 58 LNCS, 4 LNEE, 1 LNNS, 2 CCIS, and 10 IEEE proc, 4 books, EIC of IT Personnel, and Project Management, Int J of Human Capital & Inf Technology Professionals—IGI Global & editor in various SCIE journals.

Dr. Chamundeswari Arumugam is a Professor of Computer Science and Engineering Department at SSN College of Engineering, Chennai, India. Her research areas of interests include software estimation, software testing, software project management, cybersecurity, cyber forensics, machine learning, deep learning, and psychology. She has organized International conference IEEE ICCIDS 2019 and reviewed many conference paper and journal. Also she is one of the edited book authors of IGI Global. Guided many undergraduate and postgraduate students to publish research papers. Organized FDP, workshops for faculty members. She is a member of the Computer Society of India (CSI), IEEE and ACM. CSI student branch counsellor at SSN College of Engineering since 2009. She has been organizing many workshops, competitions, project colloquium, and seminars to the students, research scholars, and faculty members under the banner of SSN-CSI students chapter.