Hindawi
Security and Communication Networks
Volume 2022, Article ID 9797604, 3 pages
https://doi.org/10.1155/2022/9797604

WILEY | Hindawi

Editorial

Machine Learning and Applied Cryptography

Amir Anees,[1] **Iqtadar Hussain**,[2] **Umar M. Khokhar**,[3] **Fawad Ahmed**,[4] **and Sajjad Shaukat**[5]

[1]*La Trobe University, Melbourne, Australia*
[2]*Qatar University, Doha, Qatar*
[3]*IT Georgia Gwinnett College, University System of GA, Lawrenceville, GA 30043, USA*
[4]*HITEC University, Taxila, Pakistan*
[5]*King Khalid University, Abha, Saudi Arabia*

Correspondence should be addressed to Amir Anees; amiranees@yahoo.com

Received 30 November 2021; Accepted 30 November 2021; Published 27 January 2022

Machine learning (ML) and cryptography have many things in common, for instance, the amount of data to be handled and large search spaces. The application of ML in cryptography is not new, but with over 3 quintillion bytes of data being generated every day, it is now more relevant to apply ML techniques in cryptography than ever before. ML generally automates analytical model building to continuously learn and adapt to the large amount of data being fed as input. ML techniques can be used to indicate the relationship between the input and output data created by cryptosystems. ML techniques such as boosting and mutual learning can be used to create the private cryptographic key. Methods such as naive Bayesian, support vector machine, and AdaBoost, which come under the category of classification, can be used to classify the encrypted traffic and objects into steganograms used in steganography. Besides the application in cryptography, which is an art of creating secure systems for encrypting/decrypting confidential data, ML techniques can also be applied in cryptanalysis, which is an art of breaking cryptosystems to perform certain side-channel attacks. The aim of this special issue was to create a volume of recent works on advances in different aspects of ML applications in cryptosystems and cryptanalysis. We have selected twenty research articles which deal with different aspects of ML and cryptography.

In the paper entitled "Distributed Outsourced Privacy-Preserving Gradient Descent Methods among Multiple Parties," Z. Tan et al. presented two new outsourced privacy-preserving gradient descent method schemes over horizontally or vertically partitioned data among multiple parties, respectively. Compared to previously proposed solutions, their methods improved in comprehensiveness in a more general scenario.

In the paper entitled "Survey on Reversible Watermarking Techniques of Echocardiography," R. Ghafoor et al. presented a survey on the comparison of state-of-the-art reversible watermarking techniques. The imperceptibility and payload were balanced through a tradeoff. It has been observed in the literature that most of the reversible watermarking methods lack robustness, and very small-scale robustness has been achieved in this domain of watermarking.

In the paper entitled "Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicles: Recent Advances and Applications," E. Sayed Ali et al. provided theoretical foundations for machine learning and the leading models and algorithms to resolve Internet of Vehicles applications' challenges. This paper has conducted a critical review with analytical modeling for offloading mobile edge-computing decisions based on machine learning and deep reinforcement learning approaches for the Internet of Vehicles.

In the paper entitled "Fusion of Machine Learning and Privacy Preserving for Secure Facial Expression Recognition," A. Ullah et al. presented a novel framework and proposed an effective and robust solution for facial expression recognition under an unconstrained environment; it also helped to classify facial images in the client/server model along with preserving privacy. There are a lot of cryptography techniques available, but they are

computationally expensive; on the contrary, the authors have implemented a lightweight method capable of ensuring secure communication with the help of randomization.

In the paper entitled "Protect Mobile Travelers Information in Sensitive Region Based on Fuzzy Logic in IoT Technology," I. Memon et al. explored the possible flaws associated with security for IoT environment insensitively meant for transfer conditions. They proposed a novel design aimed at detecting a spoofing attack that inspects the probability distributions of received power found for the regions designed for mobile (moving) users.

In the paper entitled "An Improved Method to Evaluate the Synchronization in Neural Key Exchange Protocol," Y. L. Han et al. proposed an improved method for evaluating the synchronization of neural networks timelier and accurately. First, the frequency that the two networks have the same output in previous steps was used for assessing the degree of them roughly. Second, the hash function was utilized to judge whether the two networks have achieved full synchronization precisely when the degree exceeds a given threshold.

In the paper entitled "The Effect of the Primitive Irreducible Polynomial on the Quality of Cryptographic Properties of Block Ciphers," S. S. Jamal et al. introduced 16 affine power affine transformations, and, for fixed parameters, they obtained 16 distinct S-boxes. Here, they thoroughly studied S-boxes with all possible primitive irreducible polynomials and their algebraic properties. All of these boxes were evaluated with the help of nonlinearity test, strict avalanche criterion, bit independent criterion, and linear and differential approximation probability analyses to measure the algebraic and statistical strength of the proposed substitution boxes.

In the paper entitled "Towards an Improved Energy Efficient and End-to-End Secure Protocol for IoT Healthcare Applications," A. Ahmad et al. proposed local coordination Expected Message Authentication Code as an extension of Expected Message Authentication Code. Expected Message Authentication Code is an asynchronous duty cycle medium access control protocol. Expected Message Authentication Code used one important technique of short preamble which is to allow sender nodes to quickly send their actual data when the corresponding receivers wake up.

In the paper entitled "Multicriteria Decision and Machine Learning Algorithms for Component Security Evaluation: Library-Based Overview," J. Zhang et al. developed a new system based on the reusable components as reusability of components is recommended to save time, effort, and resources as such components are already made. Security of components is a significant constituent of the system to maintain the existence of the component as well as the system to function smoothly. Component security can protect a component from illegal access and changing its contents.

In the paper entitled "Evaluating Security of Internet of Medical Things Using the Analytic Network Process Method," X. Huang and Shah Nazir evaluated the security of the Internet of Medical Things by using the analytic network process. The proposed approach was applied using the ISO/IEC 27002 (ISO 27002) standard and some other important features from the literature. The results of the proposed research demonstrated the effective Internet of Medical Things components which can further be used as secure Internet of Medical Things.

In the paper entitled "Secure Framework Enhancing AES Algorithm in Cloud Computing," I. A. Awan et al. presented a framework with key features including enhanced security and owner's data privacy. It modified the 128 AES algorithm to increase the speed of the encryption process, 1000 blocks per second, by the double round key feature.

In the paper entitled "Convolution Neural Network-Based Higher Accurate Intrusion Identification System for the Network Security and Communication," Z. Gu et al. followed a deep learning-based approach for the accurate intrusion detection purposes to ensure the high security of the network. A convolution neural network-based approach was followed for the feature classification and malicious data identification purposes. In the end, comparative results were generated after evaluating the performance of the proposed algorithm to other rival algorithms in the proposed field.

In the paper entitled "Android Malware Detection Based on a Hybrid Deep Learning Model," T. Lu et al. proposed an Android malware detection algorithm based on a hybrid deep learning model which combines the deep belief network and gate recurrent unit. First, they analyzed the Android malware; in addition to extracting static features, dynamic behavioral features with strong antiobfuscation ability were also extracted. Then, they built a hybrid deep learning model for Android malware detection.

In the paper entitled "A Smart Agent Design for Cyber Security Based on Honeypot and Machine Learning," N. E. Kamel et al. presented an introduction of machine learning and honeypot systems, and based on these technologies, they designed a smart agent for cyberattack prevention and prediction.

In the paper entitled "Preprocessing Method for Encrypted Traffic Based on Semisupervised Clustering," R. Zheng et al. analyzed the differences between benign and malicious traffic produced by benign applications and malware, respectively. To fully express these differences, this study proposed a new set of statistical features for training a clustering model. Furthermore, to mine the communication channels generated by benign applications in batches, a semisupervised clustering method was adopted.

In the paper entitled "A Systematic Literature Review on Using Machine Learning Algorithms for Software Requirements Identification on Stack Overflow," A. Ahmad et al. reported a systematic literature review collecting empirical evidence published up to May 2020. This review study found 2,484 published papers related to requirements engineering and Stack Overflow. The data extraction process of the review showed that (1) latent Dirichlet allocation topic modeling is among the widely used machine learning algorithms in the selected studies and (2) precision and recall are amongst the most utilized evaluation methods for measuring the performance of these machine learning algorithms.

In the paper entitled "Deep Learning-Based Cryptanalysis of Lightweight Block Ciphers," J. So proposed a generic cryptanalysis model based on deep learning, where the model tries to find the key of block ciphers from known plaintext-ciphertext pairs. The author showed the feasibility of the deep learning-based cryptanalysis by attacking on lightweight block ciphers such as simplified DES, Simon, and Speck. The results showed that the deep learning-based cryptanalysis can successfully recover the key bits when the key space is restricted to 64 ASCII characters.

In the paper entitled "Spam Detection Approach for Secure Mobile Message Communication Using Machine Learning Algorithms," L. G. Jun et al. proposed the applications of the machine learning-based spam detection method for accurate detection. In this technique, machine learning classifiers such as logistic regression, *K*-nearest neighbor, and decision tree were used for the classification of ham and spam messages in mobile device communication.

In the paper entitled "Modelling Features-Based Birthmarks for Security of End-to-End Communication System," M. Li et al. proposed a mathematical model, which is based on a differential system, to present feature-based software birthmark. The model presented in this paper provided an exclusive way for the feature-based birthmark of software and then can be used for comparing birthmark and assessing security of end-to-end communication systems. The results of this method showed that the proposed model is efficient in terms of effectiveness and correctness for the feature-based software birthmark comparison and security assessment purposes.

In the paper entitled "Detection and Blocking of Replay, False Command, and False Access Injection Commands in SCADA Systems with Modbus Protocol," L. Rajesh and Penke Satyanarayana worked for False Command Injection attack, False Access Injection attack, and replay attacks on the Modbus protocol. Initially, a real-time SCADA test bed was set up, and they envisaged the impact of these attacks on Modbus protocol data using the test bed. They proposed and developed a method (a) to detect replay attacks by incorporating timestamp and sequence number in Modbus communications and (b) a frame filtering module which will block unauthorized attacks such as False Command Injection and False Access Injection attacks to reach PLC.

Conflicts of Interest

The editors declare that they have no conflicts of interest regarding the publication of this special issue.

Amir Anees
Iqtadar Hussain
Umar M. Khokhar
Fawad Ahmed
Sajjad Shaukat