Neural Computing and Applications (2023) 35:4809–4812
https://doi.org/10.1007/s00521-022-08183-4

EDITORIAL

Special issue on machine learning for security and privacy: advancing the state-of-the-art applications

Janmenjoy Nayak[1] · David Al-Dabass[2] · Danilo Pelusi[3] · Manohar Mishra[4]

Received: 13 December 2022 / Accepted: 13 December 2022 / Published online: 22 December 2022

In the past 10 years, several techniques have been proposed to address the security and privacy issues of smart systems. For dealing with cyber security, a set of technologies and processes designed to protect computers, networks, programs, and data from different attack, unauthorized access, change or destruction. However, smart cities are likely to increase the standard of living, endorse viable growth and improve the functionality of urban structures. Currently, several smart systems have been employed in the conventional system, which lead to a number of security and privacy issues. In this regard, the system necessitates effective countermeasures to deal with these. Based on the current applicative situations, machine learning (ML)-based algorithms have been widely employed as one of the major tools to increase the security infrastructures by improving the efficiency of intrusion detection system. Such tools have been frequently adopted to secure the Wireless sensor network of personalized decisions, secure the smart-phone, improving the biometric security systems, secure the collected data from different smart sensors, protecting the data collected from smart-meters and many more.

✉ Janmenjoy Nayak
jnayak@ieee.org

David Al-Dabass
david.al-dabass@ntu.ac.uk

Danilo Pelusi
dpelusi@unite.it

Manohar Mishra
manoharmishra@soauniversity.ac.in

1 Department of Computer Science, Maharaja Sriram Chandra Bhanja Deo University, Baripada, Odisha, India

2 School of Computing & Informatics, Nottingham Trent University, Nottingham, UK

3 Communication Sciences, Coste Sant'agostino Campus, University of Teramo, Teramo, Italy

4 Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, Siksha 'O' Anusandhan University, Bhubaneswar, Odisha, India

This special issue includes various emerging security and privacy approaches relevant to machine learning techniques which are continuously deployed for automated decisions in many real-time applications for the efficient detection of various attacks in IoT and smart systems, retrieval of images from an untrusted cloud environment, to remove unusual and redundant events recorded in videos, to eliminate illegal copying and modification of digital data by unauthorized users and to prevent image splicing forgery. Due to the advancement in computing technology, smart systems have been implemented in daily activities of life to enhance the quality of human life. The implementation of these smart systems has led to many security and privacy issues which become a challenging task when it comes to robustness and effectiveness of the system. The conventional privacy and security approaches cannot be used directly on these systems because of the heterogeneity and dynamic nature of smart systems. Nowadays, the advancement of machine learning and deep learning approaches has led to the implementation of these approaches in detection and prevention of various attacks in smart systems. This is mainly because of their strong learning abilities on massive datasets. Moreover, the performance of these algorithms in various diversified application such as IoT intrusion detection system, smart-grid systems, insecure cloud environments, video summarization, android malware detection system, intrusion detection system, image forensics, smart real estate systems, telemedical information system has also been analyzed.

Basati et al. suggested a novel intelligent network intrusion detection system known as APAE (asymmetric parallel auto-encoder) for the accurate detection of cyber-attacks in real-time IoT networks. The encoder part of APAE consists of two encoders in parallel fashion. Each of these encoders is having three consecutive layers of convolution filters. The local features are extracted in the first encoder using standard convolutional layers and a positional attention module. Whereas long range information is extracted in the second encoder using dilated convolutional layers and a channel attention module. The decoder part of APAE consists of eight consecutive transposed convolutional layers. The proposed architecture is appropriate architecture for the detection of real-time attacks because of its lightweight architecture. Moreover, the architecture provides superior performance even with limited training records. Further, the effectiveness of the suggested APAE architecture has been evaluated using three popular publicly available datasets known as UNSW-NB15, CICIDS2017 and KDDCup99 and the outcomes indicate the superiority of the suggested approach over other standard algorithms.

Chawla et al. have presented a novel cyber-attack resilient WAMS (wide area measurement system) framework to mitigate the adverse effects of cyber-attacks on smart-grid infrastructure. The inclusion of both attack detection and mitigation modules in WAMS framework ensures the resiliency of PMU (phasor measurement units) data-based supervisory protection applications. Moreover, the WAMS framework includes LSTM (long short-term memory) model for the detection of anomalies in time-series PMU measurements. The LSTM module is also used for separating the compromised PMUs followed by GAIN (generative adversarial imputation nets) to restore the compromised PMU's data. Then, the corrected PDC data-stream is sent to the decision-making end application for making the framework resilient against attacks. To differentiate fault events from other disturbances and to administer the third zone of distance for backup protection of transmission lines, a random forest classifier has been utilized in the end application. Further, the performance of the WAMS framework has been validated on the WSCC 9-Bus System modeled on a developed real-time digital simulator (RTDS)-based integrated cyber-physical WAMS testbed and the experimental outcomes indicate that the proposed WAMS framework successfully detects and mitigates the adverse effects of attacks on the end application.

Kumar et al. suggested an approach for retrieving the images securely from an untrusted cloud environment. Initially, image feature vector is formed by representing images with reference to their local invariant features. Then, the feature vector is secured by applying ASPE (asymmetric scalar-product-preserving encryption) scheme. Later, images have been encrypted before uploading to a cloud server. Further, the suggested approach has been evaluated using distinct Corel image and medical image datasets and the outcomes indicate that the suggested approach attains better performance in securing feature vector and original images during their transmission.

Yasmin et al. have developed a video summarization framework in order to summarize the activities and to eliminate unnecessary and unusual events recorded in videos. To identify informative frames, the proposed framework makes use of key moment-based frame selection and clustering of frames. Then, a similarity-based agglomerative clustering algorithm is used for partitioning the frames of video into distinct groups based on the extracted key moments. Based on the Jaccard similarity, the algorithm then finds out at most 'K' clusters, where K is a user defined parameter set as 5–15% of the size of the video to be summarized. Further, the proposed clustering algorithm and the summarization method have been assessed using standards datasets and their outcomes are compared with other related methodologies to show the effectiveness of the proposed framework.

Şahin et al. have developed a machine learning-based malware detection system for differentiating Android malware from benign applications. In the feature selection stage, the suggested malware detection system makes use of linear regression-based feature selection approach for removing irrelevant features which results in the reduction of feature vector dimension and training time of the suggested approach. Further, the proposed malware detection system has been evaluated and results indicate that the suggested system has obtained highest F measure metric of 0.961 by using at least 27 features.

Sharma et al. have presented an intelligent robust color image watermarking technique in the transform domain in order to provide security of multimedia information in the present digital world. To secure the color image, a color watermark is embedded in the color host image using singular value decomposition and discrete wavelet transform approach. To overcome the problem of digital data alteration and illegal copying by unauthorized users, additional protection is provided to the color image by scrambling information of the color watermark with a chaotic map. The extraction of watermark is done in the presence of secret key to ensure the ownership of data. Further, the scaling factor of the algorithm has been optimized using artificial bee colony algorithm to overcome the trade-off between robustness and insignificance of the proposed algorithm. Further, proposed algorithm has been evaluated and results indicate the robustness, secure and invisible nature of the proposed algorithm over other relevant watermarking schemes.

Ajij et al. introduced a novel feature set based on quasi-straightness of boundary pixel runs for verification of signature. Initially, the quasi-straight-line segments are extracted from the signature boundary pixels using elementary combinations of the directional codes. Later, a robust feature set is obtained for the signature verification from distinct quasi-straight-line classes. Further, the proposed method has been assessed on standard signature datasets known as Center of Excellence for Document Analysis and Recognition (CEDAR) and Grupo de

Procesado Digital de la Senal (GDPS-100) using support vector machine and results show that the proposed approach attained better performance over other state-of-the-art approaches.

Ozcan et al. presented a hybrid deep learning approach to prevent phishing attacks. The suggested approach makes use of deep neural network algorithms and long short-term memory for identifying phishing URL (uniform resource locator) and for assessing the model's performance on phishing datasets. Moreover, the deep connections among characters and high-level connections based on NLP (natural language processing) have been exploited and revealed using both character embedding-based and NLP feature extraction approaches. Further, experimental outcomes indicate that the suggested approach attains superior performance in terms of accuracy in comparison with other phishing detection models.

Mishra et al. have developed a novel smishing detection framework for the efficient detection of smishing using a limited number of feature set. The developed framework consists of two phases known as domain checking phase and SMS classification phase. Then, the authenticity of the URL has been examined using domain checking phase. Then, the contents of the message are scrutinized using SMS classification phase and extracts efficient features. Lastly, backpropagation algorithm has been used to classify the results. The results indicate that the suggested framework attains better performance with an accuracy of 97.93% in detecting smishing messages when compared with the other classifiers.

Keserwani et al. have recommended a comprehensive network intrusion detection system (NIDS) to maintain the reliability and effectiveness of the IDS. Initially, the authors have provided an extensive review of different IDS systems, six standard network datasets, classification approaches that makes use of machine learning and deep learning approaches and distinct dimensionality approaches for the efficient detection of intrusion in IDS. Then, the recommended NID framework has been evaluated using UNSW-NB15 dataset and the outcomes indicate that the recommended framework attains better performance of 98.11% accuracy and 97.81% detection rate in comparison with other standard approaches.

Ding et al. presented a novel image tamper location approach based on DCU-Net (dual-channel U-Net) for detecting and locating image slicing forgery in the field of forensics. The suggested approach consists of three components namely encoder, feature fusion and decoder. Initially, residual images are generated by extracting the remnants of the tampered image using high-pass filters. Then, a dual-channel encoding network model is constructed in the second stage which takes original tampered image and tampered residual image as input. Later, secondary fusion is performed by combining deep features and tampered features with distinct granularity extracted from the dual-channel encoding network and by dilation convolution, respectively. Lastly, the predicted image is decoded layer by layer by giving fused feature map as input to the decoder. Further, the suggested DCU-Net approach has been assessed using Casia2.0 and Columbia datasets and results indicate that the DCU-Net can locate tampered areas more efficiently when compared with latest algorithm. Moreover, it is concluded from the attack experiments that DUC-Net approach can also resist noise and JPEG recompression attacks.

Ullah et al. have suggested a conceptual framework for the adoption of blockchains-based smart contracts in smart cities. Initially, the authors have performed a systematic analysis of the review work carried out between 2000 and 2020 on blockchain smart contracts in smart cities. Then, the authors have highlighted ten key crucial features from the literature survey and grouped them into six layers for adoption of blockchains-based smart contracts in smart real estates. The interactions between decentralized application and Ethereum Virtual Machine (EVM) are presented to represent the development blockchain-based smart contract in real estate. Further, a stepwise procedure is presented for implementing and terminating smart contracts along with the list of functions for establishing, creating, altering or terminating smart contracts in smart real estates in order to provide a more visualized, fascinating and user-friendly contracting process.

Gupta et al. have proposed a secure authentication mechanism to verify the authenticity of user in Telecare medical information system. The originality of the transmitted message and authenticity of the user has been verified using machine learning and the nonce-based system. Further, the unauthorized access of data has been prevented using smart card blocking mechanism that has been incorporated in each stage of the proposed system. Then, the performance of the proposed mechanism has been evaluated using AVISPA tool and the results indicate that the suggested approach provides more efficiency and security when compared with other recently proposed approaches.

This special issue is dedicated with few insightful researches on various emerging security issues such as processing capability, energy consumption, interoperability, scalability, resource constraints and so on in order to stimulate more research and to provide understanding into various privacy and security issues in the smart systems among the readers, technocrats and researchers. Being the guest editors, we antedate that the range of research articles covered in this special issue will be of an asset for the researchers and technocrats working in the field of privacy and security issues in smart systems. We tried our best to

maintain the stability between the types of articles including the methodologies and their application domain in a wide range of diversity. We are obliged to the authors of this issue for their valued research contributions and supportive efforts toward the spirit for altering the paper as per the comments of reviewers. Moreover, we are grateful to the reviewer board members who have been extremely involved in providing high-quality reviews based on their expertise for the submitted papers and for maintaining the technical standards and quality of published articles in this special issue. Finally, we are thankful to the editorial members and Editor in Chief for their consistent assistance and cooperation in all possible ways for the successful accomplishment of this issue.