Journal of
Sensor and Actuator Networks

MDPI

Editorial

Blockchain and Artificial Intelligence as Enablers of Cyber Security in the Era of IoT and IIoT Applications

Mohamed Amine Ferrag [1,*], Leandros Maglaras [2] and Mohamed Benbouzid [3]

[1] Technology Innovation Institute, Abu Dhabi 9639, United Arab Emirates
[2] School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK; l.maglaras@napier.ac.uk
[3] Institut de Recherche Dupuy de Lôme (UMR CNRS 6027 IRDL), University of Brest, 29238 Brest, France; mohamed.benbouzid@univ-brest.fr
* Correspondence: mohamed.ferrag@tii.ae

check for updates

Citation: Ferrag, M.A.; Maglaras, L.; Benbouzid, M. Blockchain and Artificial Intelligence as Enablers of Cyber Security in the Era of IoT and IIoT Applications. *J. Sens. Actuator Netw.* **2023**, *12*, 40. https://doi.org/10.3390/jsan12030040

Received: 7 May 2023
Revised: 9 May 2023
Accepted: 10 May 2023
Published: 11 May 2023

The fifth revolution of the industrial era—or Industry 5.0—is the new industry trend that defines the smart factory concept. This concept is based on emerging technologies, such as 5G/6G communications, fog computing, drones, cloud computing, blockchain, artificial intelligence, deep learning, etc. To allow the optimization of operations and reduced costs, these technologies are employed to establish a connection between machines and the Internet, through the Internet of Things, and to collect information in the cloud and edge and then process them using artificial intelligence algorithms. However, with thousands of IoT-based devices deployed in the open field, there are many new cybersecurity threats in Industry 5.0. When an adversary attempts to penetrate the network, it uses several different approaches, such as DDoS attacks, scanning attacks, and false data injection attacks, to disrupt the functioning of the IoT-based devices. To protect Industry 5.0 from destruction, change, unauthorized access, or attack, security researchers propose using intrusion detection system (IDS)s or access control mechanisms combined with blockchain technology [1,2].

In recent years, many researchers have come up with proposals that took advantage of machine learning models for developing IDSs [3]. The IDS is a mechanism for monitoring network traffic, and it is used to detect suspicious or abnormal activities and then enables preventive measures for intrusion risks. The blockchain technology can be effectively applied in almost all domains of the IoT, especially when the IoT applications demand a decentralized security framework. Blockchain technology is mainly used to detect fraudulent transactions.

This Special Issue contains eight articles that focus on research and practical aspects of blockchain and artificial intelligence methods for cybersecurity. Some information about these papers follows.

The Internet of Vehicles (IoV) has gained a lot of interest as a potential research area and for its privacy and security concerns. Blockchain can ensure the IoV data's accuracy and immutability, but it cannot guarantee data privacy. Therefore, in order to preserve user privacy, IoV solutions utilizing blockchain technology must take into account adopting privacy protection mechanisms. The proposed solutions used in order to deliver various automotive services utilizing blockchain while maintaining privacy through the use of pseudonym approaches, permission management, ring signature techniques, etc., are surveyed in [4]. Identity, location, and data privacy are the three privacy issues that the authors categorise and present. They also group them based on the blockchain framework and platform that each one uses. It is discovered through classification that each distinct privacy protection field has rather mature privacy protection methods. In order to address the low latency and low computation needs of IoV, numerous blockchain-based privacy-preserving systems have started integrating other innovative technologies. Finally, the article emphasises the main issues and potential avenues for future research in this area.

The Advanced Encryption Standard (AES) 128-bit symmetric key is used by the Long-Range Wide-Area Network (LoRaWAN) to protect entities and data from various assaults. However, it is difficult to develop a universally recognised and resilient LoRaWAN security model because there are heterogeneous applications. The design of the ideal LoRaWAN security model has not yet been fully realised, despite the existence of numerous security models to maximise the security efficiency in LoRaWAN employing the trusted key server to safely manage the keys. The security models for LoRaWAN were thoroughly reviewed in [5], and two LoRaWAN algorithms were suggested as the building blocks for a more secure and advanced LoRaWAN model.

In the age of wireless communication, the Industrial Internet of Things (IIoT) is regarded as a new paradigm for executing autonomous communication in the network. However, during the sharing of information, automatic computation and data processing may introduce a number of security and privacy vulnerabilities into the system. Numerous intrusion detection systems (IDS) have been put out by various researchers, but none of them manage to identify threats with high accuracy, and they all have a significant false-positive rate. Thus, for detecting harmful behaviours taking place in the network in an IIoT environment, a novel method that combines the Viterbi algorithm and indirect trust mechanism is proposed [6]. The system's transparency is preserved by using the blockchain technology.

Many IoT address management services use Dynamic Host Configuration Protocol (DHCP), one of the most used data link layer network protocols for IP address management. A DHCP server is consequently vulnerable to a number of dangers, such as DHCP starvation dangers, DHCP dangers from rogue servers, and DHCP dangers from malicious DHCP users. In response, IPChain, a blockchain-based security protocol for IoT address management servers for smart homes, is presented in this study [7]. The proposed IPChain model employs the Diffie–Hellman key exchange mechanism, the ECDLP, a one-way hash function, blockchain technology, and a smart contract. The ECDLP was selected because it has a faster computational rate than other public key cryptosystems. The registration and validation processes make up the two main parts of the suggested model.

Alongside the rising adoption of IoT and smart devices, the transition to electronic health record (EHR) systems has accelerated in the healthcare industry. This research investigated access control recovery mechanisms for EHRs that are synchronized and exchanged among distributed healthcare providers using blockchain [8]. The authors first reviewed the current state of research on blockchain in healthcare to gain an understanding of the active areas. This was followed by narrowing the focus to research targeting blockchain in EHR systems. An analysis of current challenges in blockchain-based EHR systems and the requirements for achieving a successful access control recovery mechanism for EHRs was undertaken. Accordingly, they proposed Biometric-Based Electronic Health Record (BBEHR), a multilayer system that splits the roles between healthcare providers, the blockchain, and a cloud store.

The goal of [9] was to create a model that performed best at differentiating harmful traffic from benign traffic. To accomplish the goals of the study, a variety of feature extraction methods and machine learning algorithms were employed. The results of the studies demonstrate the significance of feature extraction methods for achieving high performance. Additionally, the Very Deep Convolutional Network entitled VGG-16 was demonstrated to have the highest accuracy and precision. The impact of individual and layered machine learning algorithms was examined in this study. It also looked into how the data split ratio affected how the models were run.

Lack of ongoing monitoring of data on vehicle performance internally and the condition of each internal component is a problem for the automobile industry's current structure. From the time a vehicle leaves the factory until its first and second uses, this information is necessary. A number of concerns, such as the history and performance of the vehicle, the originality of the modified parts, their longevity, the history of suggested maintenance, etc., become unreliable due to a lack of reliable information. In Reference [10], the authors presented a remote automatic automobile diagnosis solution. Their entire system is automated. The system's basic concepts include checking each part's performance and authenticity on a regular basis, as well as checking every Diagnostic Trouble Code (DTC) that has been recorded in the car. The system then creates a block to send to the servers of the car manufacturer. These data can be used by the manufacturer to examine how the car performs in various locations and weather situations. If necessary, they can also improve performance by modifying the software and updating it remotely using Flash Over The Air (FOTA). Additionally, the key advantage is that they can promote their goods utilising accurate data obtained from a credible source, such as the blockchain.

The last article of the Special Issue focuses on the protection of people and property as a service offered by institutions. Target tracking with camera sensor networks has drawn a lot of interest recently. In Reference [11], the authors present a method termed CRP that makes use of camera sensors' mobility to improve the cooperative operation amongst camera sensors by using a pattern recognition algorithm based on the targets' historical data. With the help of camera sensors, the cooperative relay tracking with prediction (CRP) technique creates a movement schedule to determine which camera should move, stay active, and which camera should take over the monitoring task. It then forecasts the future path of the moving item. This is compared to the Wait technique and the CR strategy, which employ unpredicted cooperation relaying.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Saidi, H.; Labraoui, N.; Ari, A.A.A.; Maglaras, L.A.; Emati, J.H.M. DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data. *IEEE Access* **2022**, *10*, 101011–101028. [CrossRef]
2. Derhab, A.; Guerroumi, M.; Gumaei, A.; Maglaras, L.; Ferrag, M.A.; Mukherjee, M.; Khan, F.A. Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors* **2019**, *19*, 3119. [CrossRef] [PubMed]
3. Pinto, A.; Herrera, L.C.; Donoso, Y.; Gutierrez, J.A. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. *Sensors* **2023**, *23*, 2415. [CrossRef] [PubMed]
4. Chen, W.; Wu, H.; Chen, X.; Chen, J. A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain. *J. Sens. Actuator Netw.* **2022**, *11*, 86. [CrossRef]
5. Ntshabele, K.; Isong, B.; Gasela, N.; Abu-Mahfouz, A.M. A Trusted Security Key Management Server in LoRaWAN: Modelling and Analysis. *J. Sens. Actuator Netw.* **2022**, *11*, 52. [CrossRef]
6. Rathee, G.; Kerrache, C.A.; Ferrag, M.A. A Blockchain-Based Intrusion Detection System Using Viterbi Algorithm and Indirect Trust for IIoT Systems. *J. Sens. Actuator Netw.* **2022**, *11*, 71. [CrossRef]
7. Yakubu, B.M.; Khan, M.I.; Bhattarakosol, P. IPChain: Blockchain-Based Security Protocol for IoT Address Management Servers in Smart Homes. *J. Sens. Actuator Netw.* **2022**, *11*, 80. [CrossRef]
8. Barka, E.; Al Baqari, M.; Kerrache, C.A.; Herrera-Tapia, J. Implementation of a Biometric-Based Blockchain System for Preserving Privacy, Security, and Access Control in Healthcare Records. *J. Sens. Actuator Netw.* **2022**, *11*, 85. [CrossRef]
9. Musleh, D.; Alotaibi, M.; Alhaidari, F.; Rahman, A.; Mohammad, R.M. Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT. *J. Sens. Actuator Netw.* **2023**, *12*, 29. [CrossRef]
10. Yassin, A.M.; Aslan, H.K.; Abdel Halim, I.T. Smart Automotive Diagnostic and Performance Analysis Using Blockchain Technology. *J. Sens. Actuator Netw.* **2023**, *12*, 32. [CrossRef]
11. Hussein, Z.; Banimelhem, O. Energy-Efficient Relay Tracking and Predicting Movement Patterns with Multiple Mobile Camera Sensors. *J. Sens. Actuator Netw.* **2023**, *12*, 35. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.