Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 2, No. 1, 2022

A Review of Security Research on the Internet of Things, Based on Artificial Intelligence and Blockchain

Ni Zhang

Faculty of Science, BSc General, University of Alberta. Edmonton, Alberta T6G 2R3.Canada
nz2@ualberta.ca

Abstract: With the rapid improvement of digital technology, the Internet of things (IoT) has become a trending development direction. Its massive data interaction capabilities have drawn researchers' attention to key security issues. This paper describes the concept of IoT, its application areas, and corresponding security problems. The use of blockchain and cryptographic algorithms is introduced, and the application of blockchain in IoT security is analyzed and discussed in detail. Drawing upon artificial intelligence, technical solutions such as using machine learning for privacy protection and intrusion detection are presented. Finally, the problems and challenges facing IoT, driven by blockchain and artificial intelligence, are discussed.

Keywords: Blockchain; Security; Artificial intelligence; IoT.

1. Introduction

The Internet of things (IoT) is a technology combined with the Internet designed to achieve cross-time and cross-territory interaction, offering substantial economic benefits and lowering labor costs while also reducing wasted resources. It is widely used in transportation, agriculture, logistics, home, healthcare, and other fields. According to the latest data reported by Statista, the number of IoT-connected devices exceeded 10 billion in 2021 and is expected to reach 30 billion by 2030. IoT is divided into three main parts, which are the perception layer, network layer, and application layer. The perception layer constitutes the various information-sensing devices that collect data. The network layer is responsible for the transmission of the collected data through network facilities such as private networks, mobile networks, the Internet, and more. The application layer entails the specific IoT solution that matches the needs of the industry by combining the needs of various fields.

2. Security Issues in Internet of Things

With the rapid development of IoT, which includes large-scale data storage and widespread data usage, privacy protection and other security issues present a significant challenge. Currently, IoT relies largely on centralized cloud servers, and interaction vulnerabilities in cloud platforms, malware, and flaws in access control permissions can easily create threats to users' data security and privacy. Similarly, centralized storage methods also present the risk of large-scale data leakage. In 2018, for instance, because of flaws in software permission restrictions, the data of more than 50 million Facebook users was compromised. Additionally, data interaction in IoT can introduce many security issues. Examples include attacks on the networks that transmit data, unreliable data nodes, and privacy breaches during data interactions.

3. Blockchain

3.1. Blockchain Background

Ever since Satoshi Matsumoto proposed the concept of Bitcoin in 2008, blockchain, the basic underlying technology on which Bitcoin relies, has received widespread attention. Blockchain, as a pan-centralized distributed ledger, authorizes trusted data and maintains data storage through a consensus mechanism between various network nodes.

3.2. Framework and Technical Characteristics

3.2.1. Framework

The underlying framework of blockchain can be divided into the application layer, network layer, and data layer the data layer is used to record or transact data through techniques such as hash functions and asymmetric encryption. After starting from the Genesis block, each subsequent block records the hash value of the previous block so that each independent block is logically connected, thus forming a blockchain. A timestamp is also added to each block, which ensures the reliability and integrity of all previous data by verifying the hash values and timestamps of each block. This procedure makes it difficult to tamper with the data [3, 2]. The second layer, known as the network layer, is a peer-to-peer networking approach in which all data is transmitted and shared between nodes. Whenever a new transaction is posted to the network, all remaining nodes in the network can obtain validation rights through a consensus mechanism. After verification, the transaction is packaged and broadcast across the network. The proof of workload is obtained through fair competition among the nodes to acquire the packing right, and it is rewarded with corresponding tokens to ensure the security and consistency of the data. Likewise, the proof of interest is obtained through packing rights by pledging tokens to prove ownership. With the Byzantine fault tolerance, the bookkeeper is elected according to the proportion of interest, and if more than two-thirds reach an agreement, the bookkeeping can be completed. Finally, the application layer focuses on non-fungible tokens (NFTs), digital currency, decentralized applications, decentralized autonomous organizations, and more, including Open Sea, Binance, Ethereum, and others. The application layer provides call interfaces for various programs, allowing the blockchain to support data interaction from multiple domains.

3.2.2. Technical Characteristics

Privacy and scalability are the technical advantages of

blockchain. With Bitcoin, users are assigned a public key and a corresponding private key. Only the input and output addresses appear for each transaction record, effectively protecting the user's information. Combined with blockchain-related cryptography, zero-knowledge proofs were proposed in the 1980s as a method of data protection, in which a clearly defined assertion is confirmed by a verifier who has no extraneous knowledge about the prover's assertion. The verifier simply confirms whether the assertion is correct or not. Currently, zero-knowledge proofs are one of the key techniques used to address privacy protection at the blockchain transaction layer. Wang et al. propose to protect user transactions by encrypting account balances and transaction information in a lightweight, homomorphic manner before data is uploaded on the chain, so that the information seen by other nodes on the chain is encrypted. Also, blockchain has good scalability; for example, slicing and chain measurement are both used to solve the problems of low transaction volume and high latency. Slicing is one of the mainstream scaling methods for the first blockchain layer, which entails slicing the whole blockchain and dividing the work. Each node is only responsible for the corresponding storage, verification, and related procedures, making it more efficient. The measurement chain, on the other hand, is derived from the main chain and ensures data security by running its own independent blockchain and uploading valuable information to the main chain on a regular basis.

3.3. IoT Security Using Blockchain Technology

Blockchain currently has a wide range of applications in IoT, involving different domains and multiple technologies, and with the appeal of significant commercial value, there is no shortage of attackers who seek to identify and steal important data nodes. The sensing devices within IoT are numerous and cumbersome, and many of them do not have supporting software for long-term maintenance. Wu et al. propose Multi-Layer Aggregate Authentication (MLAV), an efficient blockchain management framework that allows regular upgrades and system maintenance of IoT devices to defend against malware attacks. Uzair et al. discuss the use of smart contracts with an Ethereum variant that limits a single device Gas not to exceed the Gas of the smart contract, thus preventing denial-of-service attacks. Network nodes, which form an important part of the blockchain, have also gained the attention of attackers. Song et al. have designed a visual inspection tool based on IoT blockchain data to ensure the validity of data by checking if the blockchain network is functioning properly and detecting malicious nodes. Vishwakarma et al. propose a blockchain-enabled secure storage and communication scheme (BBS) that combines the tamper-resistant features of blockchain, where authenticated objects are divided into secure, trustworthy regions, where the objects can interact freely. For privacy issues associated with personal schedules, Giannoutakis et al. outline a blockchain-based decentralized architecture for the enhancement of cybersecurity in smart homes, where the IP of the home device is managed through smart contracts and the IP of the attacker is blacklisted through anomaly detection to protect the user's data. Xu et al. also suggest using smart contracts to automatically determine whether patient data, after homomorphic encryption, is eligible for health insurance claims, thus avoiding the risk of data leakage of sensitive patient information.

4. Artificial Intelligence

4.1. Background of Artificial Intelligence

Artificial intelligence (AI), a technology that mimics and extends human intelligence, is composed of a basic resource layer, a technology layer, and an application layer. AI involves data platforms, image recognition, natural language processing, driverless capabilities, and more. Presently, AI is still in a relatively weak stage in comparison to its full potential, with prominent examples including Apple's Siri, AlphaGo, and other technologies that can only handle specific scenarios. Machine learning, the core research area of AI, has a wide selection of techniques such as supervised learning, reinforcement learning, and deep learning. Supervised learning focuses on training an optimal model using known data, with the objective of mapping an input to the corresponding output using the trained model, which would thus introduce predictive power for unknown data. Reinforcement learning, on the other hand, maximizes the reward function value by recording the model's behavior based on the feedback given by the environment, which rewards or penalizes the model based on the correctness of its actions. Finally, deep learning is a technique based on neural networks that involves learning the underlying laws of data. Geoffrey et al. suggest that multilayer artificial neural networks have superior learning abilities and can overcome network training difficulties by initializing layer by layer. Because deep learning is superior at constructing complex and high-dimensional data structures, it plays an important role in natural sciences, medicine, and business.

4.2. Development and Application of Artificial Intelligence in the Field of IoT Security

4.2.1. Malware Detection

The lack of unified security protocols across IoT nodes, coupled with the embedded nature of many IoT devices, which cannot patch the latest security vulnerabilities, makes IoT technology susceptible to malware attacks. Deep learning, when used for classifying and detecting malware, can extract feature values from software code to identify whether it has been attacked, analyze it by observing the running behavior of the software, or combine these methods. Asam et al. discuss a deep learning detection framework (IMDA) that combines three features of deep learning by using the STM smoothing operation of multi-path dilation convolution to identify the full structure of the attacking malware, presenting a form of malware discrimination with an accuracy of over ninety-seven percent. Nawaz et al. propose a malware detection method based on a convolutional neural network that effectively finds malware and its variants using pre-trained deep learning models.

4.2.2. Defending Against Cyberattacks

With the continued development of IoT, the corresponding network has become huge and complex. Network transmission, as the core of IoT interaction, faces the difficulties of long concealment time, fast transmissibility, and high destructive power, among other issues that can lead to severe network attacks. Ren et al. introduce a network intrusion monitoring model based on deep reinforcement learning (ID-RDRL) that combines deep reinforcement learning features and removes eighty percent of the redundant features to identify network attacks in complex network environments. However, identification difficulties occur

when network attacks overlap with normal network traffic. Vijayakumar et al. analyze problematic and normal network IDs using convolutional neural network modeling and a hybrid hyperparameter approach; their model is more efficient than traditional machine learning, but the identification capability needs to be improved to detect new intrusion methods.

5. Conclusion

This paper describes the background and applications of the Internet of things and summarizes various security issues that have become increasingly complex and difficult to detect following the continuous development of IoT. A solution for IoT security based on blockchain and artificial intelligence is introduced. The security features of blockchain, such as its resistance to tampering, its traceability, and its anonymity are all utilized to provide a guarantee for IoT data security and safe information transmission. Combined with the advantages of artificial intelligence in multi-dimensional data analysis and detection, this security solution screens and defends against potential vulnerabilities. To a certain extent, the security of IoT is improved by using this approach. Research on artificial intelligence and blockchain in the field of IoT is still in its preliminary stage, but the future combination of reliable algorithms and efficient and stable blockchain encryption can better serve the security needs of IoT.

References

[1] Vailshery, L. S. (2022, Aug. 22). Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030 (in billions) [Graph]. Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[2] Yang, Y., Zhou, W., Zhao, S., Liu, C., Zhang, Y., Wang, H., Wang, W., & Zhang, Y. (2021). Survey of IoT security research: threats, detection and defense. Journal on Communications, 42(8), 188-205.

[3] Gao, W., Hatcher, W. G., & Yu, W. (2018). A survey of Blockchain: Techniques, applications, and challenges. 2018 27th International Conference on Computer Communication and Networks (ICCCN), 1-11.

[4] Wang, R., Tang, Y., Pei, X., & Guo, S. (2021). Block-chain privacy protection scheme based on lightweight homomorphic encryption and zero-knowledge proof. Computer Science, 48(11A), 547-551.

[5] Huang, H., Kong, W., Peng, X., & Zheng, Z. (2022). Survey on blockchain sharding technology. Computer Engineering, 48(6).

[6] Wu, J., Sie, M., Harding, S. A., Lin, C. L., Wang, S., & Liao, S. (2021). Multi-layer aggregate verification for IOT blockchain. 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 43-44.

[7] Javaid, U., Siang, A. K., Aman, M. N., & Sikdar, B. (2018, June 1). Mitigating Iot device based DDoS attacks using blockchain. CryBlock'18: Proceedings of the 1st workshop on cryptocurrencies and blockchains for distributed systems, 71-76.

[8] Song, J., Nang, J., & Jang, J. (2018). Design of anomaly detection and visualization tool for IOT blockchain. 2018 International Conference on Computational Science and Computational Intelligence (CSCI), 1464-1465.

[9] Vishwakarma, L., & Das, D. (2020). BSS: Blockchain enabled security system for internet of things applications. 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA), 1-4.

[10] Kim, J. N., Jeon, Y. S., & Han, J.-H. (2015). Security considerations for secure and trustworthy smart home system in the IOT environment. 2015 International Conference on Information and Communication Technology Convergence (ICTC), 1116-1118.

[11] Xu, W., Wu, L., & Yan, Y. (2018). Privacy-preserving scheme of electronic health records based on blockchain and homomorphic encryption. Computer Research and Development, 55(10).

[12] Hinton, G., & Salakhutdinov, R. (2006). Reducing the dimensionality of data with neural networks. Science, 313(5786), 504-507.

[13] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521, 436-444.

[14] Zhang, Y., Dong, Y., Liu, C., Lei, K., & Sun, H. (2018). Situation, trends and prospects of deep learning applied to cyberspace security. Computer Research and Development, 55(6).

[15] Asam, M., Khan, S. H., Akbar, A., Bibi, S., Jamal, T., Khan, A., Ghafoor, U., & Bhutta, M. R. (2022). IOT malware detection architecture using a novel channel boosted and squeezed CNN. Scientific Reports, 12.

[16] Newaz, S., Imran, H. M., & Liu, X. (2021). Detection of malware using deep learning. 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON), 1-4.

[17] Ren, K., Zeng, Y., Cao, Z., & Zhang, Y. (2022). Id-RDRL: A deep reinforcement learning-based feature selection intrusion detection model. Scientific Reports, 12.

[18] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). Applying convolutional neural network for network intrusion detection. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 1222-1228.