JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Overview of Residual GRU Smart Contract with One-Way Compression for IoT Attack Detection

T.Nishitha
Assistant Professor in GRIET, Hyderabad, Telangana, India

Dr.Akhil Khare
Professor of MVSR,Hyderabad, Telangana, India

Abstract

The Internet of Things (IoT) system is a complex environment where various entities and devices communicate. IoT is used in fields like transportation, healthcare, and monitoring, linking smart devices with sensors through the Internet to collect data from the physical world. To protect this sensitive data from hackers, an IoT platform or architecture that ensures end-to-end privacy and security is essential. Although there are many security and privacy solutions for IoT that offer basic security needs like confidentiality, integrity, and authentication, traditional solutions fall short for the large-scale IoT paradigm due to its heterogeneous nature and resource-constrained devices. Hence, this research focuses on decentralized architectures. Block chain (BC) technology is gaining attention for addressing security and authoritarian issues. In this approach, a block chain smart contract is updated with an attack detection contract.

Keywords: blockchain technology, one-way compression function, Miyaguchi-Preneel

Cryptographic.

1. INTRODUCTION

The Internet of Things (IoT) system is a complicated environment in which various entities and devices communicate [1]. Currently, the Internet of Things (IoT) is employed in a variety of fields such as transportation, nursing, and monitoring, wherein intelligent devices that include sensors are linked collectively through the Internet in order to gather data from the physical world [2-4]. IoT devices generate an enormous quantity of information in real time, that is saved for processing and analysis to ensure that IOT applications meet their service needs [5]. Aside from that, IoT enables advancement in a variety of fields, including home-to-smart-home, city-to-smart-city, school-to-smart-school, health-care-to-smart-healthcare, and so on. The IoT system must allow the tracking of all devices that are connected (physical or virtual), as well as the retrieval of the device's generated data by consumers from any place [6]. However, it is essential that only individuals with permission be able to access the network and its facilities. If not, it can encounter a number of security issues like data alteration, theft of identities, as well as data leaking.

The IoT data gathered in many of these applications [7] is sensitive and needs to be maintained confidential and secure. Sensitive IoT data can involve physiological data gathered by biomedical sensors that are (which is, in some situations) wearable, energy consumption data gathered by smart meters, even location data gathered by mobile phones, to mention some of them. Such information could be made public, which could lead to criminal action, severe injury, and possibly mortality. As a result, from this angle, IoT poses an enormous problem for security, privacy, and trust; these are thought to be some of the primary obstacles still standing in the way of developing IoT applications. The majority of currently available IoT privacy-sensitive data protection technologies concentrate on the security and authorization of communication channels. This gives hackers and unscrupulous administrators the chance to obtain and reveal privacy-sensitive data gathered from IoT devices.

II. MOTIVATION

Centralized security systems can be a single point of failure, making all connected devices vulnerable if breached. This underscores the need for innovative solutions like blockchain technology to tackle the unique security challenges of IoT devices. While some basic techniques have been developed to address security issues, traditional studies often use ML models such as DT, SVM, LR, ANN, and RF to identify attacks. These ML-based methods can adapt to new attack types but often require extensive training data and computational power. Some struggle with large datasets, while others fail to detect new or unknown attacks. These limitations highlight the necessity for innovative solutions like blockchain technology to secure IoT devices.

III. LITERATURE REVIEW

Han Qiu et al [13] presented SUPER-IOT, a revolutionary strategy for improving the security and efficiency of AI applications in distributed IoT systems (AIoT). This solution used the SUPER-IOT method to efficiently secure DNN model inference in AIoT systems. To fight AEs and preserve acceptable performance for clean samples, this method used three methods such as pixel dropping, pixel reconstruction, and image denoising. It performed a wavelet-based denoising operation on the model server to eliminate adversarial perturbations including misleading noises. By lowering the bit stream of sensory data given, these methods achieved high network transmission efficiency for Internet of Things applications. The network throughput must be reduced further, and this is a disadvantage that needs to be fixed using higher drop ratio and improved reconstruction methods.

In order to demonstrate the trust level confidence to external networks, Ahmad Sharafidz Khalid et al. [14] established behaviour capturing as well as verification techniques in block chain backed smart-IoT systems. To prevent faulty or fraudulent sensors within the network, a sensor-level filter which may steady output from one or more sensors was included. Each zone's Main/Master node has Behaviour Monitor established and configured, which may record and examine IoT device runtime activity. This method uses a deep learning strategy (auto-encoders) for realization on the behaviour monitor to identify the device and decide a level of trust. To secure the security and integrity of critical application code and data, each IoT-Zone has developed a Trusted Execution Environment (TEE). Nevertheless, this approach has an almost long detection time. In this research work the dataset has been collected from various sensors in the smart-home IoT network. To ensure in real-time that the training dataset is clean and not malicious, normal traffic from IoT devices are collected immediately after its joining to the IoT network.

A blockchain-based architecture was presented by Nabil Rifi et al [12] to improve wireless device security in the IoT ecosystem. In order to provide secure data access protocols, the concept included publisher-subscriber relationships, off-chain databases, and smart contracts. The blockchain served as a decentralized and secure method to safeguard IoT data access, guaranteeing the data's transparency and immutability. This is utilized to link the blockchain with complementing off-chain database technologies to handle the bulk of the data to be stored. They also presented an analytical model to examine the effectiveness of the mining process, that has an important influence on the whole system's time to react. The mining process and transaction processing times may take longer with this method, which could cause delays and bottlenecks.

IV. OBJECTIVE OF THE RESEARCH

- Enhance data security in the IoT environment by implementing a Blockchain Network.
- Effectively detect attackers in IoT using deep learning technology.
- Develop a new model with improved accuracy and precision for recognizing IoT attacks.
- Analyze the performance metrics of the proposed scheme in terms of accuracy, throughput, and time complexity.

V. RELATEDWORK

A few straightforward techniques have been created to deal with security-related issues. In addition, conventional studies usually use ML models like DT, SVM, LR, ANN, and RF to identify attacks. This machine learning-based identification can change to accommodate new attack types, but it might need a lot of training data and computer power. In a signature-oriented approach, threats and assaults have been kept in a database and reviewed at set intervals. These methods, nevertheless, incur processing fees and are susceptible to threats submitted in an anonymous way. Although these methods are frequently employed in traditional works to identify attacks, they also have certain disadvantages. For instance, some of these strategies might struggle to handle huge datasets effectively, and others might struggle to identify brand-new or undiscovered assaults. A second technique is anomaly-based detection that includes creating a baseline of typical activity for an entire network or device before spotting departures from it. If valid operations differ from the specified baseline, it could also produce false positives. Additionally, behaviour-based detection concentrates on observing user, process, or networking entity behaviour to spot nefarious or illegal activity. It entails developing models or

characteristics of typical behaviour and identifying any differences from them. This method may need a lot of computer resources but it can be useful in identifying new assaults.

Thus, to attain these goals, the following contributions are presented in this approach.

- In this approach, smart contract of blockchain is updated with the contract of attack detection.
- For attack detection, an enhanced Residual Gated Recurrent Unit (RGRU) architecture is presented.
- The performance of the proposed scheme is evaluated in terms of Confidentiality rate, Data integrity rate and Processing time.

VI. CONCLUSION

The Internet of Things (IoT) system is a complicated environment in which various entities and devices communicate. We must create an IoT platform or architecture that assures end-to-end privacy and security if we are to prevent hackers from accessing these privacy-sensitive data. There are many security and privacy-related solutions for IoT contexts that offer the fundamental security needs, such as confidentiality, integrity, and authentication. Traditional solutions, however, are unable to satisfy the desired security requirements in the forthcoming large-scale IoT paradigm due to its heterogeneous nature and possessing lower resource devices. Despite the efficiency and security of some security-based solutions, these solutions frequently rely on centralized procedures. Therefore, the focus of this research is on decentralized architectures. Blockchain (BC) technology is attracting a lot of attention for its ability to address issues with security, confidentiality, tracking, and authoritarianism.

References

1. Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), pp.1645-1660.
2. Fan, Q. and Ansari, N., 2018. Application aware workload allocation for edge computing-based IoT. IEEE Internet of Things Journal, 5(3), pp.2146-2153.
3. Yan, H., Li, X., Wang, Y. and Jia, C., 2018. Centralized duplicate removal video storage system with privacy preservation in IoT. Sensors, 18(6), p.1814.
4. Jhaveri, R.H., Patel, N.M., Zhong, Y. and Sangaiah, A.K., 2018. Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT. IEEE Access, 6, pp.20085-20103.
5. Wang, T., Bhuiyan, M.Z.A., Wang, G., Rahman, M.A., Wu, J. and Cao, J., 2018. Big data reduction for a smart city's critical infrastructural health monitoring. IEEE Communications Magazine, 56(3), pp.128-133.
6. Hammi, M.T., Livolant, E., Bellot, P., Serhrouchni, A. and Minet, P., 2018. A lightweight mutual authentication protocol for the IoT. In Mobile and Wireless Technologies 2017: ICMWT 2017 4 (pp. 3-12). Springer Singapore.
7. Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I., 2012. Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7), pp.1497-1516.
8. Komninos, N., Philippou, E. and Pitsillides, A., 2014. Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials, 16(4), pp.1933-1954.
9. Nakamoto, S. and Bitcoin, A., 2008. A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 4(2).
10. Mettler, M., 2016, September. Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom) (pp. 1-3). IEEE.
11. Yuan, Y. and Wang, F.Y., 2016, November. Towards blockchain-based intelligent transportation systems. In 2016 IEEE 19th international conference on intelligent transportation systems (ITSC) (pp. 2663-2668). IEEE.
12. Rifi, N., Rachkidi, E., Agoulmine, N. and Taher, N.C., 2017, September. Towards using blockchain technology for IoT data access protection. In 2017 IEEE 17th international conference on ubiquitous wireless broadband (ICUWB) (pp. 1-5). IEEE.
13. Qiu, H., Zheng, Q., Zhang, T., Qiu, M., Memmi, G. and Lu, J., 2020. Toward secure and efficient deep learning inference in dependable iot systems. IEEE Internet of Things Journal, 8(5), pp.3180-3188.
14. Ali, J., Khalid, A.S., Yafi, E., Musa, S. and Ahmed, W., 2020. Towards a secure behavior modeling for iot networks using blockchain. arXiv preprint arXiv:2001.01841.
15. Jayaraman, P.P., Yang, X., Yavari, A., Georgakopoulos, D. and Yi, X., 2017. Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation. Future Generation Computer Systems, 76, pp.540-549.

16. Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S.A. and Shekhar, S., 2018, April. Continuous security in IoT using blockchain. In 2018 IEEE international conference on acoustics, speech and signal processing (ICASSP) (pp. 6423-6427). IEEE.