International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Scalable Architectures for Embedded Systems in IoT Environments

G.Lingeswaran[1], Dr.A.Babu Karupiah[2], Mr.R.V.Ashokprathap[3], Mr.R.Rajaraja[4]

Assistance Professor,Department of Electronics and Communication Engineering, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Morur (Post), Sankari (Tk), Salem, lingeswarang@shanmugha.edu.in

Professor, Department of Electronics and Communication Engineering, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Morur (Post), Sankari (Tk), Salem, babukarrupiah.ece@shanmugha.edu.in

Assistance Professor, Department of Electronics and Communication Engineering, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Morur (Post), Sankari (Tk), Salem, Ashokprathap@shanmugha.edu.in

Assistance Professor, Department of Electronics and Communication Engineering, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Morur (Post), Sankari (Tk), Salem, rajaraja.ece@shanmugha.edu.in

Abstract- Internet-of-things (IoT) is perpetually revolutionizing our daily life and rapidly transforming physical objects into an ubiquitous connected ecosystem. Due to their massive deployment and moderate security levels, those devices face a lot of security, management, and control challenges. Their classical centralized architecture is still cloaking vulnerabilities and anomalies that can be exploited by hackers for spying, eavesdropping, and taking control of the network. In this paper, we propose to improve the IoT architecture with additional security features using Artificial Intelligence (AI) and blockchain technology. We propose a novel architecture based on permissioned blockchain technology in order to build a scalable and decentralized end-to-end secure IoT system. Furthermore, we enhance the IoT system security with an AI-component at the gateway level to detect and classify suspected activities, malware, and cyber-attacks using machine learning techniques. Simulations and practical implementation show that the proposed architecture delivers high performance against cyber-attacks.

Keywords – Internet-of-Things, Blockchain, Cyber Security, Machine Learning, IoT architecture.

INTRODUCTION

Internet-of-Things (IoT) technology has become highly auspicious to enhance automation, efficiency, and comfort level for users. Indeed, the number of IoT devices has widely increased. It is expected to exceed 8.4 billion devices in 2020 and reach 20.4 billion devices in 2022 engendering a tremendous amount of traffic and data sharing among data providers and consumers[1]. Although IoT technology proved its efficiency in different fields and became essential in many applications such as healthcare, remote monitoring, smart homes, and smart agriculture, it remains under continuous upgrades and does not reach its maturity yet[2]. The IoT environment is indeed still vulnerable and can be controlled by hackers who can use moderate

security levels of hardware as well as firmware vulnerabilities to control those devices for espionage and eavesdropping. Often, data leakage takes place during transmission, share, or storage of data, which may entail serious problems for the IoT owners and This paper is accepted for publication in IEEE Technology & Engineering Management Conference (TEMSCON'20), Detroit, USA, jun. 2020. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. Users[3]. Indeed, usually, IoT devices acquire basic security and authentication levels. From this perspective, some researchers suggested blockchain-based solutions so as to reinforce the authentication and identification processes as well as data encryption and sharing. However, those suggestions are not immune against hackers cyber-attacks who execute malware and exploit device vulnerabilities to achieve their goals. Moreover, the connected devices can be used and monitored by hackers and cybercriminals to create sophisticated cyber-attacks which may lead to dangerous and fatal consequences[4]. Recently, Mirai malware used IoT devices and targeted Domain Name Service (DNS) servers in order to generate a sophisticated Distributed Denial of Service (DDoS) attacks which affected the internet service for a large number of users such as Netflix, GitHub, and Reddit and causes huge losses for those companies. One of the most effective means to secure IoT devices and services is providing an end-to-end secure IoT architecture and uncircumventable access control for IoT devices. Artificial Intelligence (AI) has been widely used in many industrial domains for its efficiency in upgrading IoT devices with sophisticated smart features[5]. In this context, we propose a novel architecture for IoT devices combining blockchain and AI technologies not only in order to decentralize data storage and protect shared data into the IoT network but also to enhance its performance and efficiency against malware and cyber-attacks. This work investigates the power of machine learning techniques as well as the efficiency of blockchain technology in order to improve privacy, data sharing, and security for IoT devices and smart city infrastructure which are vulnerable and can be used for sinful activities. We advocate the use of the permissioned blockchain to share and store the IoT devices data for its compatibility in IoT distributed architecture, where unlike some suggested approaches, the connected devices do not participate in the mining process and decision-making due to their limited computation power[6]. Then, we apply machine and deep learning algorithms such as Artificial Neural Networks (ANN), XGBoost, decision tree, and naive bayes for malware detection and classification, running on nodes participating in the blockchain network to control and detect suspicious activities. Our simulation results illustrate the efficiency of the proposed architecture for IoT privacy, data sharing, and malware detection into the proposed[7].

RELATED WORK

In this section, we discuss some of the state-of-art techniques and technologies applied to IoT systems while highlighting the novelty of this work with respect to existing studies. A system integrating blockchain, Service-oriented Architecture (SoA), and Key Performance Indicator

(KPI) was suggested by W. Viriyasitavat et al. to ensure data validity and deal with the heterogeneity, uncertainties, and mobility of devices. Blockchain was also applied in for data sharing into multiple distributed parties in industrial IoT. Federated learning was integrated in consensus process of the blockchain to build data models and share them into the blockchain network[8]. Liu et al. developed a shared data architecture based on blockchain technology and deep reinforcement learning for Industrial IoT devices. A decentralized architecture based on permissioned blockchain was suggested in order to share and secure the circulating data in smart city infrastructure. Hyperledger Sawtooth was utilized to overcome the infrastructural challenges for the smart city deployment[9]. In addition, a supplemental module was developed to automate and reduce the blockchain deployment processes. The previous solutions may provide a generic architecture for IoT services and integrate different cutting-edge technologies. However, they are unable to protect the IoT environment and the blockchain network from hackers who may control the network by bypassing the moderate hardware security and exploit vulnerabilities in IoT firmware to achieve their atrocious activities. In order to emulate IoT services, a machine learning approach was suggested by M. Pahl et al. based on interservice communication observations[10]. They developed an inter-service communication model for micro-services analysis between different IoT devices. In addition, they suggested a continuous correlation algorithm for different observations within the IoT devices. Trust list model was suggested by K. Kataoka et al. to automate the verification and trusting of IoT devices and services [6]. In this context, a trust list presenting a distributed trust between the different IoT-related stakeholders is developed. In this architecture, blockchain and software-defined network (SDN) were integrated to automate and enforce the IoT authentication processes as well as circulating the trusted IoT services and devices along the different stakeholders presented in the network. An IoT malware detector for large-scale networks was proposed. A machine learning algorithm is executed on the user access gateway in order to detect the suspicious activities based on patterns scanning traffic. Additionally, a policy module was developed to determine the needed actions for malicious packets[11]. Moreover, a database was applied to store the scanned patterns in order to update or receive them when needed. A malware detection architecture was developed for android IoT devices. In this architecture, machine learning techniques were applied to extract malware information received from an android device and store them into a blockchain network. The blockchain stores the malware features and share them into the distributed ledger. M. Shen et al. suggested Paillier public-key crypto system in order to encrypt and protect the data provided from IoT devices. In addition, they implemented the support vector machine (SVM) algorithm to train the machine learning model directly from the blockchain network[12]. Data provided from the IoT device is encrypted then saved and distributed on different distributed ledgers. Although the previous studies suggested some malware detection approaches based on intelligent systems and machine learning techniques, they were unable to guarantee the authenticity and the integrity of data transmitted from the IoT devices into the IoT network. In fact, the architecture of typical IoT environments relies on brokered communication models, which have limited scalability and

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

are exposed to multiple vulnerabilities due to the centralized authority for identification, authentication, and storage[7].

PROPOSED ARCHITECTURE

The proposed architecture is essentially built on the idea of exploiting AI and blockchain advantages to design a more robust and resilient system ensuring high-level of security and scalability. Typical public blockchain solution presents multiple draw-backs which keep it far away of being used for generic IoT platforms due to the limited resources and computation power of IoT devices. In fact, this limitation prevents those devices from being effective miners in the blockchain network[8]. Also, due to the massive deployment of those devices and their basic security levels, the blockchain network can be manipulated if more than half of these nodes were accessed by unauthorized entities. For those reasons, we propose to employ a novel permissioned blockchain network architecture combined with AI technologies as illustrated in Fig. 1. In traditional IoT environment, hackers may exploit firmware and hardware vulnerabilities present in gateways, servers, and IoT devices such that they can manipulate them and use their amassed power to achieve different cyber-attacks such as DDos which may lead to temporary denial of service in the network. However, in the proposed architecture, AI modules integrated in the IoT environment can detect suspicious and abnormal activities occurring in the network as well as protect those devices from different cyber-attacks. IoT devices submit their data to gateways which are also considered as nodes participating in the blockchain network with other servers and nodes sharing the same IoT network. Submitted information are verified, validated, and integrated into the network by authorized nodes. Also, the proposed solution ensures a blockchain based architecture for all devices and nodes participating into an IoT environment as well as the ability to extend and connect this network to other blockchain or any external network[9]. The proposed architecture ensures decentralization, high scalability, and good performance thanks to the permissioned blockchain features as well as sufficient security levels, malware, and cyber-attacks detection ensured by the efficient AI modules implemented into all blockchain nodes. The malware detection module is performed on IoT gateways and nodes participating into the blockchain network[10]. This assumption ensures early and real-time detection as well as reduces the risk to any cyber-attack attempt for the blockchain network or any malware execution from the IoT devices or between the network nodes.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

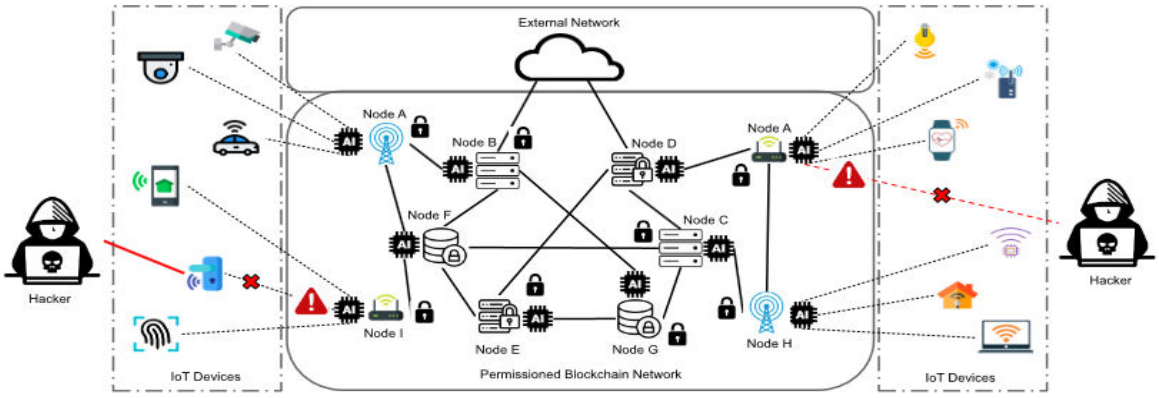

Figure 1- Artificial intelligence and blockchain based architecture for heterogeneous IoT system[4]

PERMISSIONED BLOCKCHAIN FOR IOT NETWORK

A blockchain is a growing, distributed, and immutable time-stamped data records that are linked using cryptography, managed, and distributed over different nodes participating in that network. Originally, blockchain was designed to record transactions for cryptocurrency systems. However, the use of this technology has been widely extended and used in many other fields such as industry and healthcare. In literature, there are two major types of blockchain architecture: permissioned and permission-less blockchain networks, based on the application scenario, transactions types, and access rules[6]. Also, different blockchain platforms were developed such as Ethereum, Ripple, and Hyperledger to emulate the blockchain architecture, mining process, and the access re- strictions for users. In permission-less blockchain, aka public blockchain, any-one can join the blockchain network, submit transactions, participate in the mining process, and leave the network without any restriction or permission needed in advance11]. This type of architecture ensures an open and decentralized data sharing network between all nodes participating into the blockchain. Moreover, all submitted transactions should be verified and validated before creating the block and being integrated into the blockchain. This process is ensured by a consensus protocols. Usually, in public blockchain, the Proof-Of-Work (PoW) consensus mechanism is used to validate transactions and create new blocks to the chain. For permissioned blockchains, sets of rules are defined and shared between all nodes participating into the blockchain network in order to control access and manage this network[12]. In fact, this type of blockchains is considered more secure and restricted compared to the public one. Commands and management rules are not authorized for all nodes participating into the network, but they are assigned to certain set of trusted nodes which have these authorities. Miners are also authorized nodes in the network and they are the only entities that have the authority to create, validate, and integrate new blocks into the blockchain. Practical Byzantine Fault Tolerance (PBFT) is the commune consensus protocol for this type of blockchain. The PBFT algorithm is an improvement of the BFT[8], which has the ability to be run in

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

asynchronous environment and also ensures high-speed transaction processing while solving the Byzantine general problems. For privacy and efficiency concerns, we advocate the use of a permissioned blockchain, more precisely, the hyperledger fabric which is an implementation of distributed ledger technology that ensures high level of security, scalability, and performance. This type of permissioned system ensures strong identity management between different IoT nodes, distinguishes between users and validators, and affects each user its exact role into the network. In fact, hyperledger fabric provides a membership identity service that controls member IDs and authenticates users participating into the blockchain network. Access and permission rules provide an additional security layer for the proposed IoT network, where these devices can participate into the blockchain network with restricted authorities and control to minimize data leakage from the IoT devices. In addition, thanks to its modular design[7], this system presents better performance and scalability, where data submission requires less validation time while maintaining decentralized storage and better security and privacy levels. Nevertheless, this architecture is not sufficient to protect the network from malware and cyber-attacks especially the ones initiated through IoT devices. Therefore, we add another layer of security based on AI and machine learning to cope with those problems unsolved by permissioned blockchain[10].

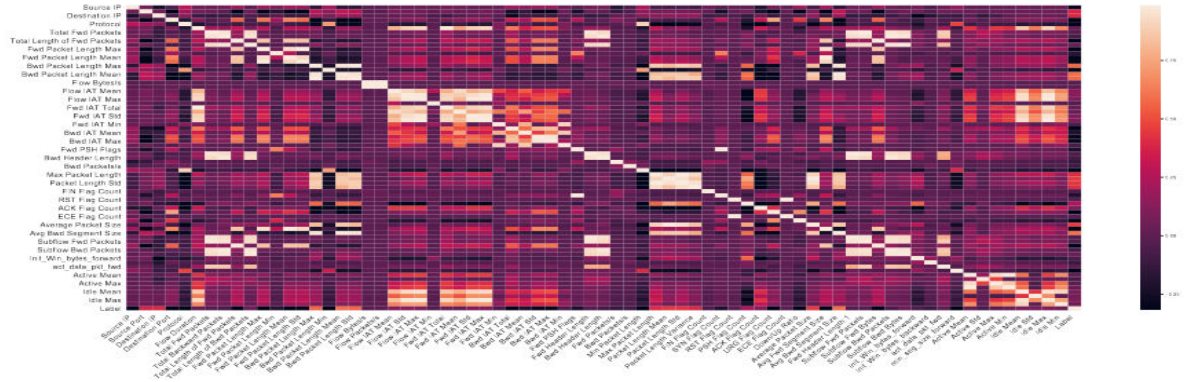

Figure 2- Correlation heat-map matrix for the selected features[6]

CONCLUSION

In this study, we introduced a novel architecture for IoT networks based on blockchain and AI technologies to decentralize authorities, enhance data sharing, and protect them from cyber-attacks. Due its compatibility with the distributed nature of IoT systems, we employed permissioned blockchain to share and store the IoT devices data. Then, we supported edge and back-end entities with AI modules where machine and deep learning algorithms such as ANN and decision tree-based algorithms are implemented to detect and classify suspicious activities in the blockchain network. Through implementation and simulations, we evaluate the efficiency of the proposed architecture in detecting and classifying cyber-attacks using practical and real-world datasets where decision tree based models show better performance compared to other state-of- the-art algorithms. As a future work, we aim to strengthen the proposed architecture by

other AI modules capable of not only detecting and classifying cyber-attacks but also automatically recovering and helping make cyber-attack response decisions.

REFERENCES

[1]. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," IEEE Access, vol. 7, pp. 82 721–82 743, June 2022.

[2]. A. Bader, H. Ghazzai, A. Kadri, and M. Alouini, "Front-end intelligence for large-scale application-oriented Internet-of-Things," IEEE Access, vol. 4, pp. 3257–3272, 2022.

[3]. Y. Jin, M. Tomoishi, K. Fujikawa, and V. P. Kafle, "A lightweight and secure IoT remote monitoring mechanism using DNS with privacy preservation," in IEEE Annual Consumer Communications Networking Conference (CCNC'19), Las Vegas, NV, USA, January 2022.

[4]. T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in IEEE Technology Engineering Management Conference (TEMSCON'17), Santa Clara, CA, USA, June 2022.

[5]. Sanjay Kumar Suman, Dhananjay Kumar and L. Bhagyalakshmi, "Non Cooperative Power Control Game with New Pricing for Wireless Ad hoc Networks", International Review on Computers and Software, vol. 9, no. 1, pp. 18-28, 2014. ISSN: 1828-6003,

[6]. S. Porselvi, Sanjay Kumar Suman and L. Bhagyalakshmi, "Harvesting RF energy for mobile charging", Australian Journal of Basic and Applied Science, vol. 9, no. 20, pp. 454-465, June 2015.

[7]. K. Swapna, P. Rajalakshmi and Sanjay Kumar Suman, "Security Enhancement in MANET using Game Theory", Middle East Journal of Scientific Research, vol. 23, pp. 190-195, 2015.

[8]. Sujeetha Devi, Bhagyalakshmi L and Sanjay Kumar Suman, "Cluster based energy efficient joint routing algorithm for delay minimization in wireless sensor networks", International Journal of Pure and Applied Mathematics, vol. 119, no. 15, 307-313, 2018

[9]. Sujeetha Devi, Bhagyalakshmi L and Sanjay Kumar Suman, "Enhancing the Performance of Wireless Sensor Networks through Clustering and Joint Routing with Mobile Sink", International Journal of Engineering and Advanced Technology, vol. 8, issue 6, pp. 323-327, 2019. https://doi.org/10.35940/ijeat.E7664.088619

[10]. L. Bhagyalakshmi, Sanjay Kumar Suman, S. Mohanalakshmi, and Satyanand Singh, "Improving Spectral Efficiency and Coverage Capacity of 5G Networks: A Review", Advances in mathematics: scientific journal, vol.9, no. 6, pp. 3387-3397, 2020. https://doi.org/10.37418/amsj.9.6.19

[11]. R. Dagar, S. Som, and S. K. Khatri, "Smart farming – IoT in agriculture," in IEEE International Conference on Inventive Research in Computing Applications (ICIRCA'18), Coimbatore, India , July 2022.

[12]. K. Kataoka, S. Gangwar, and P. Podili, "Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN," in IEEE World Forum on Internet of Things (WF-IoT'18), Singapore, Singapore, February 2022.

[13]. R. Wang, W. Tsai, J. He, C. Liu, Q. Li, and E. Deng, "A video surveil- lance system based on permissioned blockchains and edge computing," in IEEE International Conference on Big Data and Smart Computing (BigComp'19), Kyoto, Japan, February 2022.

[14]. M. Singh and S. Kim, "Trust bit: Reward-based intelligent vehicle commination using blockchain paper," in IEEE World Forum on Internet of Things (WF-IoT'18), Singapore, Singapore, February 2023.

[15]. C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, July 2022.

[16]. L. Chan, I. Morgan, H. Simon, F. Alshabanat, D. Ober, J. Gentry, D. Min, and R. Cao, "Survey of ai in cybersecurity for information technology management," in IEEE Technology Engineering Management Conference (TEMSCON'19), Atlanta, GA, USA, June 2022.

[17]. M. Muslih, Somantri, D. Supardi, E. Multipi, Y. M. Nyaman, A. Ris- mawan, and Gunawansyah, "Developing smart workspace based IoT with artificial intelligence using telegram chatbot," in IEEE Interna- tional Conference on Computing, Engineering, and Design (ICCED'18), Bangkok, Thailand, September 2022.

[18]. S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in IEEE International Conference on Advanced Communica- tion Technology (ICACT'17), Bongpyeong, South Korea, 2022.