World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:18, No:4, 2024

Enhancing IoT Security: A Blockchain-Based Approach for Preventing Spoofing Attacks

Salha Alshamrani, Maha Aljohni, Eman Aldhaheri

***Abstract*—**With the proliferation of Internet of Things (IoT) devices in various industries, there has been a concurrent rise in security vulnerabilities, particularly spoofing attacks. This study explores the potential of blockchain technology in enhancing the security of IoT systems and mitigating these attacks. Blockchain's decentralized and immutable ledger offers significant promise for improving data integrity, transaction transparency, and tamper-proofing. This research develops and implements a blockchain-based IoT architecture and a reference network to simulate real-world scenarios and evaluate a blockchain-integrated intrusion detection system. Performance measures including time delay, security, and resource utilization are used to assess the system's effectiveness, comparing it to conventional IoT networks without blockchain. The results provide valuable insights into the practicality and efficacy of employing blockchain as a security mechanism, shedding light on the trade-offs between speed and security in blockchain deployment for IoT. The study concludes that despite minor increases in time consumption, the security benefits of incorporating blockchain technology into IoT systems outweigh potential drawbacks, demonstrating a significant potential for blockchain in bolstering IoT security.

***Keywords*—**Internet of Thing, Spoofing, IoT, Access control, Blockchain, Raspberry pi.

I. Introduction

THE fast spread of IoT devices has led to significant changes in various industries, from manufacturing and healthcare to everyday applications. However, the networked nature of these devices and their susceptibility to different cyber threats and assaults pose substantial security difficulties. Among these risks, the integrity and security of IoT systems are particularly vulnerable to spoofing attacks, which involve pretending to be a reliable network or device to gain access, alter data, or interfere with operations. To address these security challenges, blockchain technology has emerged as a promising tool for boosting the security and reliability of different applications, including IoT [1].

Blockchain provides a distributed, immutable ledger that ensures transaction transparency, data reliability, and resistance to tampering. Implementing blockchain technology in IoT frameworks can establish a robust, secure structure that minimizes the potential for spoofing attacks. Moreover, this technology can be employed for the storage of sensor data, management of device settings, and facilitation of micro-transactions in IoT infrastructures. Furthermore, blockchain technology eliminates the need for third-party verification, positioning it as an efficient security protocol tailored for the computational and memory requirements of IoT devices [2].

The utility of blockchain technology extends to the healthcare sector, where it can enhance the security of medical systems' information. It can also help address security challenges in Fog computing, a platform that offers IoT, networking, storage, and computing services. Blockchain technology can offer solutions to bolster security, helping to fend off potential attacks on IoT systems.

These solutions can be leveraged to design a variety of blockchain systems and security tools [3]. This study attempts to investigate how blockchain technology might be used to combat spoofing attacks on IoT systems. The goal is to create a trustworthy intrusion detection system that uses blockchain technology to improve security and stop unwanted access. It is possible to have a thorough understanding of the difficulties and possibilities related to blockchain and IoT security by researching the existing literature and related studies. The study will examine the benefits and drawbacks of blockchain technology in relation to the IoT, particularly with regard to guarding against spoofing attacks. It will look at the viability of incorporating blockchain into IoT networks and assess how it will affect system performance, taking into account elements like time delay and resource usage. The proposed solution involves developing a blockchain-based IoT architecture and implementing a reference network to simulate real-world scenarios. In-depth tests and simulations will be used in the research to evaluate the efficacy of the blockchain-based intrusion detection system. The system's performance will be measured using metrics like time, security, and resource utilization, and it will be compared to those of conventional IoT networks without blockchain. The findings of this study will improve the understanding of how to use blockchain technology to protect IoT systems from spoofing attacks. The outcomes will provide insight into the practicality and efficacy of employing blockchain as a security mechanism as well as throw light on the trade-offs between speed and security in blockchain deployment for IoT.

II. Exploring Blockchain Technology for Enhancing IoT Security

Blockchain technology has been experiencing significant interest in recent years, emerging as a potential answer to enhancing security within IoT systems, with a particular focus on mitigating the issues associated with spoofing attacks. A

Salha Al-Shamrani is with University of Jeddah, Saudi Arabia (e-mail: 2100288@uj.edu.sa).

multitude of studies have delved into the application of blockchain within the sphere of IoT security [4]-[6]. A pivotal study [7] in this field has proposed an innovative blockchain-based IoT architecture, which facilitates distributed access control as well as data management. The authors of this study have accentuated the necessity to transition away from the traditional centralized trust model and instead, bestow data ownership upon the users. By leveraging blockchain technology as a verifiable and distributed access control layer, their architecture guarantees secure data sharing coupled with robust access control management. Furthermore, the system permits the storage of IoT time series data at the network's edge through a locality-aware decentralized storage system. This research serves as a critical cornerstone for further exploration into the advantages of decentralized access control and secure data sharing within IoT environments [7].

Blockchain technology can be utilized in several ways to improve the security of IoT systems. Specifically, each IoT device, upon installation and connection to the blockchain network, would possess a unique GUID and paired symmetric key. This eradicates the necessity for key distribution and management. Consequently, streamlined security protocols are adopted that align with the computing and memory requirements of IoT devices. Blockchain ensures the integrity of stored approved transactions and can be implemented within IoT to record sensor data, administer device settings, and facilitate micro-transactions [8].

Blockchain technology, through its inherent characteristic of eliminating the need for third-party verification, serves as an efficient security protocol that aligns with the computational and memory resource requirements of IoT devices. The application of blockchain technology in the sphere of IoT security has been explored in various studies [5], [6]. For instance, a system predicated on the fusion of IoT, blockchain, and Interplanetary File System (IPFS) for enhancing data management security was proposed in one such study. This system employs blockchain methodology to securely store batch and streaming information emanating from an array of wearable devices, devised to capture medical indicators in real-time. Moreover, the utility of blockchain technology extends to addressing security challenges within Fog computing - a platform that offers a host of services such as networking, storage, and computing, in addition to IoT. By presenting security enhancement solutions, blockchain technology is capable of thwarting potential security threats within IoT systems. These solutions can be harnessed for the creation of a variety of blockchain systems and security tools [9].

Further research has delved into the improvement of security and dependability by integrating blockchain technology with the IoT. It has been understood that the stringent hardware requirements imposed by a blockchain network could create difficulties in accomplishing a smooth integration with IoT [10]. However, it has been noted that IoT can still leverage the advantages of blockchain technology through APIs offered by network nodes or specialized intermediaries [11]. Such characteristics can significantly augment the security of IoT systems by promoting secure data sharing among internet-connected devices. An extensive discussion has been put forth by researchers on the burgeoning issue of blockchain cybersecurity, suggesting blockchain as a prospective remedy to address the security issues tied to IoT. This exploration underscores the potential application of blockchain technology as an additional layer of protection for IoT devices [12].

The security challenges intrinsic to cloud-enabled IoT applications have been meticulously explored. It has been noted that IoT applications exhibit heavy reliance on cloud computing for services, affordable applications, and data storage, which in turn, calls for the execution of stringent security measures. A particular focus has been laid on the security issues that arise from resource-constrained devices such as sensor networks, which struggle with cryptographic key generation due to their limited resources. The necessity of addressing the prevalent security issues in cloud-enabled IoT applications has been highlighted through in-depth research and literature analysis. This investigation underscores the importance of robust security measures and the unique security challenges faced by IoT applications that are reliant on cloud computing [13].

Access control to data embodies two critical elements: authentication and authorization. Authentication serves to verify the identity of the individual seeking access to the system, and subsequently grants them prior authorization. However, even after an individual gains access, it is essential to define the data they can interact with since each person is assigned specific permissions based on their role. If an unauthorized individual were to gain access to sensitive data within an organization, the implications could be devastating. This situation is amplified when considering data access via the Internet, implying the possibility of remote access to the data. We consider a scenario where the data pertain to financial transactions, such as access to a bank account. In this instance, a plethora of information about the account holder becomes accessible, including their IP address, login details, and passwords. If these data were to fall into the wrong hands due to a cyber breach, it could pose a serious threat to the individual's financial security, and the risk of identity theft becomes a persistent concern. The complexity of Internet-based access and the prevalence of open networks exacerbate the challenge of maintaining strict access control. This complexity underscores the necessity for robust and dynamic security protocols, particularly in environments such as the IoT, where data interaction is often intricate and wide-ranging. Hence, effective access control mechanisms become crucial in safeguarding against unauthorized access and ensuring the integrity and security of data within IoT systems [14].

The issue of data management in cloud-enabled IoT applications is a significant one. Specifically, the process of acquiring, processing, and managing master data presents numerous technical requirements. As IoT applications expand, so does the emergence of big data challenges, with massive quantities of data being exchanged through cloud services. Over recent years, the use of IoT applications has become widespread, especially within business operations. It has thereby necessitated the organization, storage, and integration of these data – a fundamental aim for any institution utilizing

IoT technology. One key aspect in this regard is cloud storage auditing, which is the process of validating the authenticity of data shared among a group of users in the cloud. A feature of these auditing schemes is user revocation – the process of removing a user's access rights – due to various reasons including changes in group membership. In earlier methods, the computational overhead for such revocations was directly proportional to the total number of file blocks owned by the revoked user [15].

Nonetheless, given the significant amount of data shared through the cloud, this overhead can become challenging. It brings up a significant research issue—how to lessen the computational load of user revocations while preserving the integrity of cloud data auditing. As a solution, a novel storage auditing technique has been put forward. The proposed methodology facilitates a streamlined process for user revocation in cloud computing environments, exhibiting scalability irrespective of the quantitative magnitude of file blocks possessed by the revoked user. This is made possible through a distinctive key generation procedure and a new private key updating mechanism. Rather than adjusting the revoked user's authenticators, the private keys of the group's non-revoked users are updated, leading to a more streamlined revocation process. The application of this method and technique holds potential for enhancing the efficiency and security of cloud data management in IoT applications [16].

Collectively, these related works contribute towards a deeper understanding of the potential of blockchain technology in fortifying IoT security and mitigating the risks associated with spoofing attacks. Various facets such as access control, data management, cloud integration, and network security within the context of IoT systems are explored [17]. While the benefits of blockchain technology are acknowledged, these studies also recognize the challenges associated with its deployment, including stringent hardware requirements, limitations of resources, and the inevitable trade-off between security and performance. The valuable insights offered by these studies lay a solid foundation for future research and exploration into the utilization of blockchain for preventing spoofing attacks and ensuring a secure environment for IoT.

III. Proposed Solution and Methodology

A. Proposed Solution

The proposed solution in this research focuses on enhancing the security of IoT systems through the utilization of blockchain technology. The methodology employed involves the development of two IoT systems - one without blockchain and one with blockchain - which are tested using the MQTT protocol. The objective is to investigate how blockchain can enhance the security features of an IoT system. In the initial phase, a smart home environment is set up using IoT devices, where data are collected and transmitted to a smart watch and smartphone for display. This communication is facilitated using the MQTT protocol without the integration of blockchain technology. The data are shared on a specific topic, allowing the smart watch and smartphone to subscribe and receive information from the IoT devices.

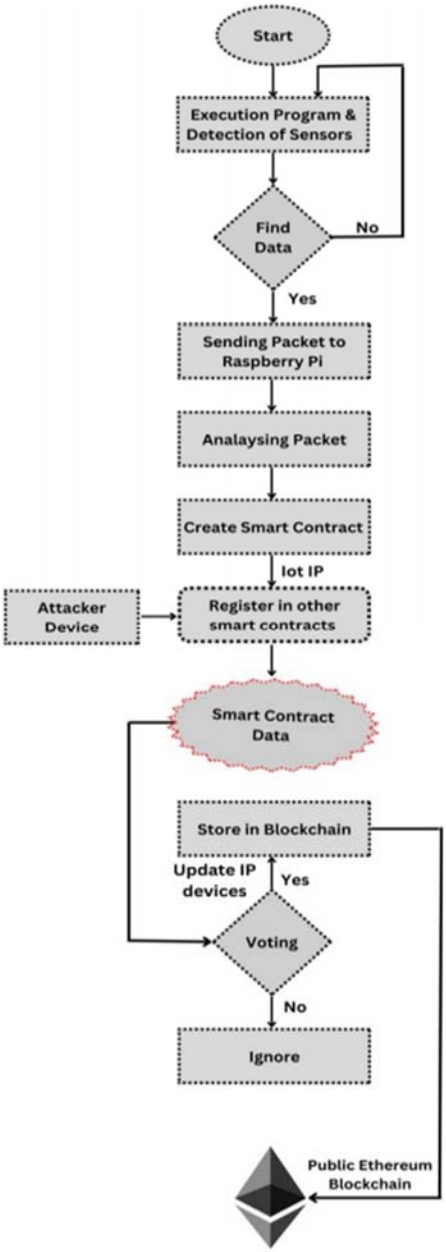

Fig. 1 Flowchart of attack IoT system with blockchain

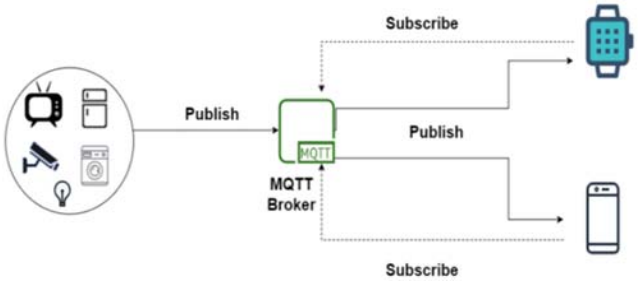

Fig. 2 IoT System without Blockchain Technology

Fig. 3 IoT System using Blockchain Technology

Conversely, the second stage encompasses the substitution of the MQTT protocol with a blockchain network and a smart contract. This amalgamation allows for secure communication amongst numerous IoT devices, with the smart contract functioning as an intermediary for data storage and retrieval from the blockchain network. Smart contracts, once implemented on the blockchain, ensure the inalterability of the code and require thorough testing and debugging during the developmental stage. To measure the efficacy of the suggested solution and evaluate the resources of the IoT system, a Raspberry Pi is deployed both with and without a malicious node. The research adheres to a sequence of steps, commencing with the formation of a reference network using a Raspberry Pi with a single primary node and three devices without any harmful nodes. Resource consumption data are collected from this network. Following this, a compromised leaf node, symbolizing a spoofing attack, is incorporated, and additional resource consumption data are collected. The contrast between the resources utilized by the spoofing attack and the standard reference network validates the necessity of adopting blockchain technology in the proposed solution.

Following the evaluation of the affected network with spoofing attacks, the research proceeds to simulate a reference network without malicious nodes using a small number of nodes and different sensors. The simulation is conducted using a Raspberry Pi simulator, and data packets from the simulator are analysed using various metrics such as packet overhead, delivery ratio, average end-to-end delay, inconsistencies, loops, and network path stretch. These metrics are employed to assess and evaluate the effectiveness of the proposed model in countering spoofing attacks and enhancing the security of the IoT system.

B. Methodology

To fulfil the primary objective of developing a robust intrusion detection system for IoT devices, and to comprehensively evaluate the system resources, we strategically incorporated the use of a Raspberry Pi in our methodology. The Raspberry Pi was utilized in different scenarios, either with the presence of a malicious node or without it, based on the specific requirement of the test scenario.

We initiated the process by constructing a reference network employing a Raspberry Pi, comprising one main node and three subsidiary devices. This initial setup was designed without the integration of any malicious nodes. The primary intent of this step was to accumulate a foundational dataset regarding the utilization of system resources under normal conditions. The choice of a relatively small number of leaf nodes was intentional, driven by the consideration to expedite the result generation process. Following the successful establishment of the reference network, we introduced an anomaly in the form of an infected leaf node, often referred to as a Spoofing Attack, into the model. Subsequently, data related to system resource utilization was collected and analysed. As per our anticipation, we observed that the resource consumption associated with the spoofing attack significantly exceeded that of the normal reference network.

Given these findings, we made an informed decision to utilize blockchain technology to construct our model, considering its inherent properties that offer enhanced security and transparency. In the final step of our methodology, we executed a re-simulation of the affected network, introducing spoofing attacks one at a time.

Furthermore, we will delve deeper into the operational environment of our proposed model that aims to combat spoofing attacks. This exploration involves the use of a Raspberry Pi as a simulator. We will commence by testing a simulated reference network devoid of any malicious nodes, restricting our initial test to three nodes equipped with varied sensors. Our decision to limit the node count is predicated on our belief that a simulation of a larger network would necessitate excessive resources, potentially complicating the process. For the simulation, we will rely on the default parameters of the Raspberry Pi simulator, validated by extensive evaluation in previous studies. Utilizing data packets procured from the Raspberry Pi, we will leverage various performance metrics to assess and evaluate the effectiveness of our proposed model.

TABLE I
DATA PACKETS FROM RASPBERRY PI

Time	Temp (C)	Humidity %
7:10:5	27.60	62.2
7:10:20	27.90	59.0
7:10:37	28:30	57.5
7:11:8	29:20	52.0

In the assessment phase of our proposed model, various performance metrics will be employed. Among these are packet overhead, which refers to the total count of control packets in the system, and delivery ratio, a measure of the proportion of successfully received data packets at the root node relative to the total data packets generated by all nodes in the network. Another critical metric is the average end-to-end delay, signifying the meantime duration taken for packets from individual nodes to successfully reach the root node, excluding

those packets which are lost or dropped. It is worth noting that delays may be induced due to processes such as blockchain mining and voting mechanisms. We will also monitor for inconsistencies, which represent the count of packets received by a node that were intended for a descendant but also originate from a child node. Similarly, we will track loops, which are those packets that not only show inconsistencies but also have their flag activated.

Further, we will consider network path stretch, defined as the ratio of nodes with path stretches exceeding one. Here, path stretch refers to the disparity between the actual cost of a node's route and the cost of the shortest possible path. Once the model is fully developed and the proposed solution is integrated, we will commence the testing phase. In this step, the effectiveness of the model will be evaluated based on key performance parameters such as accuracy and speed. This rigorous evaluation process will ensure that the final solution delivers optimal results in real-world scenarios.

This research primarily focuses on two key objectives. First, we outline the creation process of a reference network, employing blockchain technology and Raspberry Pi. Secondly, we dive into the implementation of spoofing attacks. We elaborate on the attack strategy across three distinct nodes, followed by detailing how blockchain technology plays a role in resolving the issue at hand.

1) *IoT Operating System Simulation:* The heterogeneity of sensors and the rapid evolution of IoT devices contribute to the diversity of IoT operating systems, as depicted in our proposed solution. Consequently, it is imperative to choose a platform that aligns with the project goals and objectives. For our experiments, we employed a Raspberry Pi to simulate the IoT operating system and its sensor array. Specifically, we used a Raspberry Pi version 3B+, equipped with 1GB memory, an extended 40-pin GPIO header, 16GB storage, and a power input of 5V/2.5A. The selected operating system for our Raspberry Pi was Raspbian.

Fig. 4 Raspberry Pi version 3 model B+

2) *Utilized OS:* Raspbian is a freely available operating system developed on the Debian framework, specifically tailored for the Raspberry Pi hardware. It forms the core of basic programs and utilities, enabling the Raspberry Pi to function seamlessly. However, Raspbian extends its capabilities beyond just providing an operating system. It comes with over 35,000 packages, which are essentially pre-compiled software programs packaged in a user-friendly format for effortless installation on a Raspberry Pi. By opting for Raspbian OS in our Raspberry Pi, we ensured a robust foundation to simulate the IoT operating system, essential for our proposed solution. The integration of blockchain technology in this setup facilitated the effective detection and resolution of spoofing attacks, reinforcing the IoT system's security. Our endeavour to simulate this environment aimed to substantiate the effectiveness of our proposed model in a controlled environment, resonating with our overarching research objective of enhancing IoT security.

3) *Procedure:* In order to replicate the functionality of a wireless sensor node, the Raspberry Pi proves to be a highly effective tool. It allows us to build and fine-tune an operating system (OS), which can then be used to construct a simulated real-world scenario based on the real-time output from the OS. The steps to simulate a wireless sensor network using a Raspberry Pi are as follows:

1. Initialize the Raspberry Pi by setting up the Raspbian OS: The Raspberry Pi boots up with the Raspbian OS, a Debian-based operating system that is optimized for the Raspberry Pi hardware. This step is integral to establishing a functional base for the sensor network simulation.
2. Install sensors on Raspberry Pi: The next phase involves integrating various sensors into the Raspberry Pi. This allows the system to monitor and gather data pertaining to a wide range of parameters, thus effectively mimicking the sensor node in a real-life scenario.
3. Reading and processing data from sensors: Once the sensors are installed and activated, they start gathering data on their assigned parameters. This could involve monitoring parameters such as temperature and humidity. The data collected are then processed to determine the appropriate action based on predefined parameters.
4. Setting up spoofing attack: After the sensor nodes have been set up, the next step involves initiating a spoofing attack. This process simulates an intruder's attempt to breach the security of the IoT network by disguising as a legitimate device.
5. Installing and implementing Blockchain: The final step involves setting up a blockchain network using the Ethereum platform. This platform was chosen due to its suitability for developing the model within a secure and critical environment. The tools we use include Ganache and Truffle. Ganache is a personal blockchain utilized for Ethereum application development, deployment, and testing. Truffle, on the other hand, provides a comprehensive suite of tools that serve as a development environment, a testing framework, and a MetaMask wallet. Together, these tools allow us to develop, test, and implement secure Ethereum applications, thereby bolstering the security of our IoT network against spoofing attacks.

By walking through these steps, we can successfully emulate the operation of a wireless sensor network, observe the repercussions of a spoofing attack, and assess the effectiveness of blockchain technology as a countermeasure.

IV. Results and Discussion

The collected data from the preliminary phase of the experiment showcased the reference network's aptitude to fulfil its intended operations adequately. Despite demonstrating commendable security measures and completing tasks within the predicted timeframe, the network was found to be deficient in features to mitigate spoofing attacks, rendering it susceptible to unauthorized device incursions. During the second phase, the proposed blockchain-based system was integrated for the purpose of assessing its efficacy in obstructing spoofing attacks. The outcomes from this phase illuminated the system's capability to detect and counteract unauthorized devices attempting to access the network, thereby significantly enhancing the security measures. However, this heightened security was accompanied by a minor delay in task execution. The final phase incorporated a node executing a spoofing attack into the reference network, along with the installation of the proposed blockchain system. The objective was to evaluate the system's effectiveness in preventing the attack. The results ascertained the system's success in thwarting the spoofing attack, thereby effectively reducing the risk of unauthorized network access.

The experiments involving the proposed system validated its efficacy in deterring spoofing attacks and elevating overall network security. Despite a slight delay in task completion attributed to the augmented security measures, the advantages of improved security overshadowed the minor reduction in efficiency. The evidence from this research suggests that blockchain-based systems can significantly enhance IoT networks by bolstering security and safeguarding against unauthorized access. The experiments, as delineated in Table II, aimed to simulate a fictitious attack on the reference network. To ensure data reliability, the experiment was conducted four times, each lasting 10 minutes in real-time. The experiment configuration involved five nodes, with four acting as client nodes transmitting test packets to the server every four seconds. Primarily, the goal was to measure the network's resource consumption, thereby prohibiting any attacker activity or spoofing. The network was constituted of a server and four client nodes. The resulting data showed that the time required to sum all sensor data is depicted in Table III.

TABLE II
Time of Each IoT without Using Blockchains

Experience n	IoT1	IoT2	IoT3
Exp1	12	15	10
Exp2	15	17	10
Exp3	12	15	11
Exp4	14	19	10
Exp5	16	14	14
Exp6	12	16	16
Exp7	14	19	14

TABLE III
Time of Each IoT using Blockchains

Experience n	IoT1	IoT2	IoT3
Exp1	20	23	23
Exp2	22	24	23
Exp3	23	23	21
Exp4	20	24	22
Exp5	25	25	21
Exp6	26	24	23
Exp7	24	26	24

The experiment outcomes across multiple instances for the three IoT devices have been systematically represented in Table I. It records the completion times for seven different experiments conducted with IoT devices 1, 2, and 3. The table illustrates the variation in completion times across different experimental runs and among different IoT devices, providing crucial insights into their performance under varying conditions. Subsequent experiments that replicate a spoofing attack on the reference network, as outlined in Table I, reveal a slight increment in resource utilization. These experiments were conducted in real-time over a span of 10 minutes, ensuring the reliability of the collected data. This experiment configuration encompassed five nodes, with four acting as client nodes dispatching test packets to the server at a frequency of every four seconds. These experimental constraints were designed to focus on quantifying the network's resource usage, strictly disallowing any attacker activity or spoofing. The network consisted of a server and four client nodes.

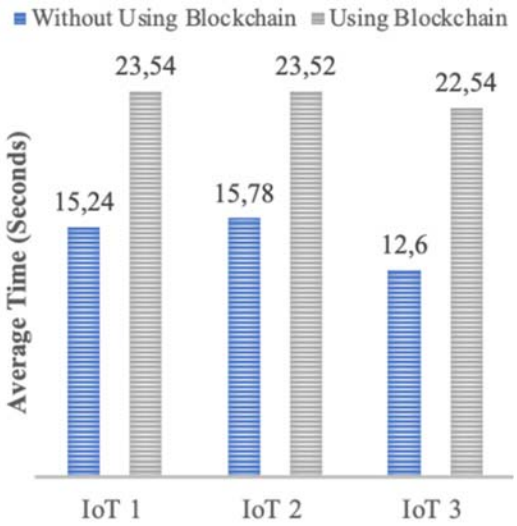

Fig. 5 Influence of using Blockchain on IoT devices

The graph showcased in Fig. 5 elucidates that IoT devices necessitate an average duration ranging between 13 to 16 seconds to complete tasks in a standard setting. The primary aim of this experiment is to gauge the amount of time and security, thereby determining how many resources are appended by integrating blockchain technology with the IoT setup.

This experiment, for its conduct, utilizes an identical structure and components as were used in experiment 1 of the

preceding section. However, it introduces a significant change – instead of the MQTT protocol, it leverages blockchain technology. This experiment remains devoid of any cyber-attacks on the network. Instead, the prime focus here lies in assessing the influence of the system on the network's overall functioning and resource usage. The objective that this experiment aims to fulfil is to ascertain whether the incorporation of blockchain amplifies the time and security aspects, and to what extent. The figure portrays that the aggregate time consumed in summing up all the sensor readings through blockchain is equal.

As illustrated in Fig. 5, the mean time, expended on tests performed on Internet of Things (IoT) devices, employing blockchain technology, is observed to range from 22 to 25 seconds. It indicates that integrating blockchain into IoT devices escalates the average time by almost 42%. Although this amplification in time might appear substantial, it is deemed justified when considered in light of the augmented safeguard against potential cyber threats.

The research methodology employed a simulator to conduct an extensive set of 100 experiments with five Raspberry Pi, sensors, and various other integral components. We categorized these experiments into three distinct phases to assess our proposed solution's efficacy under different circumstances, focusing on two crucial parameters: time and security. The first phase encompassed two key experiments. The first experiment employed a reference network to establish a baseline for comparison. This was followed by the integration of blockchain technology in the second experiment. The data derived from these experiments pointed towards a critical conclusion: our proposed solution involves a significant time overhead. However, this overhead is considered justified given the added layer of security it provides. During the third phase, we conducted three significant tests, one of which was specifically designed to evaluate our approach's resilience against spoofing assaults. Thanks to the application of blockchain technology, our solution demonstrated a high degree of efficiency in detecting attacks, registering a high rate of true positives. It is important to note that while our solution exhibits a 42% time overhead when juxtaposed with the reference network, it displays an almost 95% greater total network security overhead than the reference network. In the absence of our proposed solution, the security quotient of the reference network stands at a mere 50%. Hence, despite the increased time consumption, the enhanced security provision justifies the inclusion of blockchain in the IoT network structure.

V. Conclusion

The increasing pervasiveness of IoT devices has accentuated the importance of security in these systems. As the number of IoT devices continues to rise, the risks associated with spoofing attacks, unauthorized access, and data tampering become more prevalent. This research aimed to address these concerns by integrating blockchain technology into IoT systems to provide enhanced security. The research began by developing two IoT systems – one without blockchain and one with blockchain – and testing them using the MQTT protocol. The data collected from these systems revealed that the blockchain-integrated IoT system displayed a significantly heightened security level, effectively detecting and countering spoofing attacks. Despite a minor delay in task execution due to the enhanced security measures, the benefits of increased security clearly outweighed the minor decrease in efficiency. In the final phase, a spoofing attack was introduced into the reference network to evaluate the blockchain-integrated IoT system's effectiveness in preventing the attack. The results confirmed that the system successfully thwarted the attack, effectively reducing the risk of unauthorized network access. Overall, this research provides compelling evidence that blockchain-based systems can significantly enhance IoT networks by bolstering security and safeguarding against unauthorized access. Despite a minor increase in time consumption, the benefits of a secure network justify the inclusion of blockchain technology in IoT systems. Future work could look into optimizing the blockchain integration process to further improve the system's efficiency without compromising on security.

References

[1] S. Singh, A. S. M. S. Hosen, and B. Yoon, “Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network,” IEEE Access, vol. 9, pp. 13938–13959, Jan. 2021, doi: 10.1109/access.2021.3051602.

[2] H.-N. Dai, Z. Zheng, and Y. Zhang, “Blockchain for Internet of Things: A Survey,” IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/jiot.2019.2920987.

[3] N. Khan and M. A. Chishti, “Security Challenges in Fog and IoT, Blockchain Technology and Cell Tree Solutions: A Review,” Scalable Computing: Practice and Experience, vol. 21, no. 3, pp. 515–542, Aug. 2020, doi: 10.12694/scpe.v21i3.1782.

[4] S. Ahmed and M. Khan, "Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the IoT ecosystem," AI, IoT and the Fourth Industrial Revolution Review, vol. 13, no. 9, pp. 1–17, 2023.

[5] A. Valencia-Arias, J. D. González-Ruiz, L. Verde Flores, L. Vega-Mori, P. Rodríguez-Correa, and G. Sánchez Santos, "Machine Learning and Blockchain: A Bibliometric Study on Security and Privacy," Information, vol. 15, no. 1, p. 65, 2024

[6] Oh, J., Choi, Y., & In, J. (2023). "A conceptual framework for designing blockchain technology enabled supply chains," International Journal of Logistics Research and Applications, pp. 1–19.

[7] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, Towards Blockchain-based Auditable Storage and Sharing of IoT Data. 2017. doi: 10.1145/3140649.3140656.

[8] N. Tariq et al., “The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey,” Sensors, vol. 19, no. 8, p. 1788, Apr. 2019, doi: 10.3390/s19081788.

[9] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, “BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security,” Egyptian Informatics Journal, vol. 23, no. 2, pp. 329–343, Jul. 2022, doi: 10.1016/j.eij.2022.02.004.

[10] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing security and privacy issues of IoT using blockchain technology," IEEE Internet of Things Journal, vol. 8, no. 2, pp. 881–888, 2020.

[11] E. J. Scheid, T. Hegnauer, B. Rodrigues, and B. Stiller, "Bifröst: a modular blockchain interoperability API," in Proceedings of the 2019 IEEE 44th Conference on Local Computer Networks (LCN), October 2019, pp. 332–339.

[12] S. K. Singh and S. Kumar, “Blockchain Technology: Introduction, Integration, and Security Issues with IoT,” in Apple Academic Press eBooks, 2021, pp. 3–26. doi: 10.1201/9781003231332-2.

[13] S. D. Babar, A. Stango, N. R. Prasad, J. Sen, and R. Prasad, Proposed embedded security framework for Internet of Things (IoT). 2011. doi: 10.1109/wirelessvitae.2011.5940923.

[14] R. Lyda and J. Hamrock, “Using Entropy Analysis to Find Encrypted and

Packed Malware," IEEE Security & Privacy, vol. 5, no. 2, pp. 40–45, Mar. 2007, doi: 10.1109/msp.2007.48.

[15] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," Journal of Network and Computer Applications, vol. 67, pp. 99–117, May 2016, doi: 10.1016/j.jnca.2016.01.010.

[16] M. Cui, D. Han, J. Wang, K.-C. Li, and C.-C. Chang, "ARFV: An Efficient Shared Data Auditing Scheme Supporting Revocation for Fog-Assisted Vehicular Ad-Hoc Networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15815–15827, Dec. 2020, doi: 10.1109/tvt.2020.3036631.

[17] Salama and Barhoom, "Using Blockchain Technology to Prevent Spoofing Attack in IoT Environment," The Islamic Universityof Gaza, Aug. 2021, (Online). Available: https://blog.ajsrp.com/wp-content/uploads/2021/10/Using-Blockchain-Technology-to-Prevent-Spoofing-Attack-in-IoT-Environment.pdf