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

Maintaining IoT Data Integrity through Blockchains

Prabhakar Reure[1], Gangaprasad Patil[2], Deepak Wankhade[3], Dr. P.G. Chilveri[4], Mrs. T.A. Mate[5]

[1]Student, Department of Electronics and Telecommunication SKNCOE,SPPU Pune, India, [2]Student, Department of Electronics and Telecommunication SKNCOE,SPPU Pune, India, [3]Student, Department of Electronics and Telecommunication SKNCOE,SPPU Pune, India, [4]Associate Professor, Department of Electronics and Telecommunication SKNCOE,SPPU Pune, India, [5]Asst. Professor, Department of Electronics and Telecommunication SKNCOE,SPPU Pune, India,

Abstract— **The Internet of Things corresponds to the merging of services and external atmosphere, digitizing and connections everything, creating a productive communication interface infrastructure among both entities, items and individuals, individuals and the wider environment, and incorporating different information technologies into group dynamics through innovative service configurations in order to obtain a greater percentage of complete and thorough implementation of information surplus in human civilization. The data acquired by these sensors is extremely vulnerable to tampering or alteration. This is owing to the fact that these devices are constrained in terms of processing power and energy. As a result, an effective and lightweight technique for increasing the privacy and security of data acquired by Internet of Things sensors is required. This research article demonstrates the proposed methodology through the use of Internet of Things Devices and the generated sensor data that is effectively secured using the Blockchain Framework with regular integrity checks using Bilinear Pairing. The experimental evaluation has been performed to ascertain the effective performance of the approach which resulted in highly satisfactory results.**

Keywords— ***Blockchain, Internet of Things, MD5, Bilinear Pairing***.

I. INTRODUCTION

The Internet is a network of technologies and equipment that are linked together. The Web, as we understand it, evolved into a communications networks that went further than just connecting individuals. The very next logical stage is to register a new age known as the Internet of Things, in which the World wide web has evolved into a technology enables connectivity to a network of physical objects.. These items are equipped with solution that permits them to communicate with and interface with both our natural and manmade surroundings. The Internet of Things (IoT) is a network system that links many devices, equipment, and software solutions together. The Internet of Things (IoT) improves human existence and is an important aspect of today's modern urban environment, which is replete with mobile gadgets and technology. Hundreds of billions of sensors make up the Internet of Things, which can perceive, exchange, comprehend, and possibly actuate. The Internet of Things entails using the computers to search, analyze, and operate numerous devices and sensors. Smart homes are an excellent example of an Internet of Things implementation.

Smart smoke detectors, air pollutants monitors, smart buzzers, and household surveillance systems, among other domestic gadgets, may now connect with wearable technology and fitness trackers. A fitness tracker can notify your wakeup timer to go off after assessing your activity and determine that when you're in light slumber. The alarm system, in collaboration with your smartphone, will examine the weather immediately before you start waking up, depending on your preferences and sleeping pattern, and instruct your device and house air conditioning units to regulate the temperature appropriately. After obtaining information through your weather forecast, navigational applications on the smartphone can forecast how the climate will effect congestion problems and create a daily commute.

Because confidential and vital data may be transmitted amongst Internet of Things devices, every IoT-based system must satisfy stringent security criteria. A multitude of privacy activities, including such identification, authorization, and integrity of information, are required to build up a secure route connecting multiple devices, including an air quality monitor and a wearable device. The focus of this survey is to design effective security techniques for Internet of Things devices, as access control is a precondition for these strategies.

Computer hackers potentially penetrate Internet of Things systems because they are resource restricted and ad-hoc in construction. This highlights the importance of doing innovation in order to construct a secure and reliable Internet of Things infrastructure that can address issues and avoid assaults. Numerous assaults, particularly DoS attempts, are gaining access to the system without authorization. Because the assault targets Internet of Things sensors, removing the danger and bringing the item back operational is a difficult task. The analysis of DDoS vulnerabilities in the IoT context shows that typical network security methods like cryptography and penetration testing are insufficient for system stability.

To clarify, cryptography and infiltration identification ignore sensing and actuation observations, as well as their compliance with Internet of Things sensory processes and regulatory mechanisms, which are critical to the security system. Traditionally, the difficulty with IoT systems remained that they were only resilient to guard themselves against a specific form of assault. If the infrastructure were to have been subjected to a coordinated attack, it would be rendered essentially unusable, and the infiltration operations will indeed swiftly collapse the IoT system. Data encryption verification is especially successful in persistent processing and assessment for IoT cybersecurity owing to the excessive network and sensory data created by IoT equipment and software.

Blockchain technologies are a new foundation for managing corporate operations including such supply administration and asset life-cycle monitoring throughout enterprises. The internet of things can provide essential inputs to certain operations, such as Location information or environmental parameters such as air temp, moisture, altitude, physical stress or impact, and tremors, as well as monitoring shipping information and meteorological parameters. For example, cold-chain surveillance may be performed by introducing a temperature probe in a cargo container send its measurements to a blockchain-based SCM solution on a periodic basis. To be willing to authenticate the measurements, the recipient has to be able to consistently recognize the device and confirm that the measurements were not tampered with on their route to the blockchain.

The blockchain paradigm was created to be used in the creation of a digital notary or other services that need the time stamping of data documents. This is because the blockchain architecture is capable of preventing any changes to information after it has been recorded on the blockchain. This is accomplished by the creative application of hash identifiers. When this was first established, the blockchain would not garner much traction and was shortly overlooked. Researchers' attention in the blockchain network, which could be used to offer appropriate authentication and encryption acquired from Internet of Things smart objects, has been revived as a result of the above.

This research paper's Literature Review section portion looks at past work. Section 3 digs more into the methodology, whereas Section 4 emphasizes on the examination of the result. Section 5 concludes this study and offers some suggestions for further research.

II LITERATURE REVIEW

Ibrahim a. Abd el-Moghith [1] proposes a trustworthy networking approach that combines extensive blockchain and Markov assessment procedures to increase routing network performance. Each routing operation is approved by validators prior to getting published to the public blockchain, and the researchers use the blockchain unit to symbolize the routing information. Networking nodes will be capable of monitoring active and reliable routing information on the public blockchain via keeping individual routing transaction tracker verifiable and tamper-resistant. The MDP paradigm was also created with the goal of ensuring quick route discovery and avoiding routing ties to adversarial nodes. According to the basis of empirical evidence, the suggested schema is competent of efficiently eradicating hostile node assaults, and the device's delay is remarkable.

Shintaro Mori [2] the report's purpose is to design an anti-tamper buffering technique, as per author. The sensor nodes are distributed in a fragmented monitoring area that is separated into various zones, with a central base station coordinating overall administration. UAVs collect atomic data from Sensor Nodes and store it in a block. A candidate block, which has not yet been validated yet, is cross-checked by UAVs acting as volunteer validators. A candidate block can indeed be considered confirmed if it has adequate support from practically every credible UAV. Because the suggested methodology does not require thorough mining-based computations for block verification, it is ideal for WSN systems with minimal resources.

Rong Wang [3] According to this concept, any machine connected to the Internet can contribute in calculations and verification. However, there are drawbacks of poor quality and reduced effectiveness in the real implementation procedure. Blocks and transaction latencies are common, as are unique implementations that are not permitted in some instances. A permissioned BC is something that is administered by many organizations, which together operates one or more units. Polling, bookkeeping, and components are restricted to nodes alone. Participants connect to the network by consent and form a stakeholder affiliation to collectively preserve the functioning of the BC. Each node in the BC generally has a respective entity or organization; participants join the network by approval and form a stakeholder partnership to cooperatively sustain the operation of the BC. Only the data permits multiple organizations in the system to access, edit, and execute transactions, as well as store transaction data in a shared database. It has the following benefits: fast transaction velocity, no requirement for mining, cheap transaction fees, and supervisory assistance.

Gero Dittmann [4] envisions a blockchain integrated identity and access management based on PKI. The blockchain registers a PKI certification authority, constituting it as an identifier recognized by the blockchain members. The Certification Authority gives an identity certificate to an Internet - Of - things sensor that signs its blockchain operations with the verified private key. The sensor delivers the signed transactions, together with their certificates, to the blockchain proxies, which uses the blockchain peers to perform the needed procedures to commit the transactions to the blockchain. Reorganizing an Internet of Things unit in the environment is costly and, dependent on the equipment and use case, will not always be achievable. The Certification Authority's Internet of Things identification can last a long time and be deployed on several blockchains. The information captured from one sensor may be mapped to multiple processes over time by the receiver blockchain.

Sung-Jung Hsiao [5] use hardware components that are sensors for parameters like as temp, moisture, and quality of air. The study employs a variety of microcontroller-device methods to measure environmental data as well as associated artificial intelligence algorithms for basic information filtering. Following basic sorting, the information is categorized into classifications and saved in a relational database with a cloud-end interface. Using the Python and JavaScript computer languages, the approach additionally runs data to investigate and then translates the information into real-time webpage graphics. The suggested system may then provide a statistical representation based on the sensor information. The suggested system which allows a remote operator to access the system and observe the outcomes at the same time. Because the data from these sensors is retrieved using browser internet apps, this solution is not limited toward any mobile processors operating system.

Abena Primo [6] discusses how authentication procedures in networking have been used to decide how units connect with one another. Authentication methods are important because they influence how accessible and failure resistant a network will be, which are also both important properties of sustainability. Information on the status of the blockchain network is transferred between units in blockchain networks to preserve confidentiality without the need for a private entity. Nodes employ consensus techniques to determine the current configuration of the blockchain. As a result, a low-latency compromise technique can help boost performance. Proof-of-Work, Proof-of-Stake, and Byzantine Fault Tolerant Resolution are examples of consensus mechanisms used in public blockchains.

Alexander D. [7] The authors have focused on monitoring pairwise linear correlations among both camera image forecasting to accommodate various viewpoints, because environmental circumstances will often introduce visual discrepancies at the single-camera level, but chronological correlation values between camera systems with intersecting field - of - view ought to be stagnant under normal circumstances, according to the author. For the sake of simplification, the investigators also considered camera placements with positive correlation picture projections, employees can focus on finding abnormal discrepancies across cameras. The concept was also shown in a replicated physical surroundings, where networked virtual sensors were targeted at a shared kinetic scene from various perspectives. The suggested approach was proven to correctly identify the sensor which had been hacked following a training phase of watching baseline behavior accompanied by the subverting of a sensor. This method allows for automatic reactions to hijacked image sensors, such as denial of shared services and resources.

Sidra Malik [8] to overcome the element of concern connected with commodity integrity and organizations logging transaction records, a trust evaluation architecture for blockchain-based distribution network operations was developed. The TrustChain architecture makes use of a consortium blockchain to monitor supply chain contacts and automatically give trust management ratings based on such connections. The architecture also helps to the creation of a reputation system that is both agency and resource oriented, can allocate product-specific reputation to the very same user, and uses smart contracts to accomplish standardization and effectiveness. With regard to dangers in recommender systems, the researchers conducted a qualitative vulnerability study. The extra cost caused by Trustchain is small, according to a performance evaluation of a working prototype application using Hyperledger.

Mohammed Hayman Salih Mohammed [9] explains that as the Internet of Things (IoT) grows in popularity and networks are more accurately implemented, the requirement for protecting communications across IoT nodes is becoming increasingly important. To solve the issues, a reliable, autonomous agent-based approach that accomplishes both massive safe mode and the needed efficiency must be devised. In this work, a novel hybrid technique for preserving security in Internet of Things systems employing blockchain technology is described. The Ethereum PoS protocol has been used in the first phase to detect DoS attacks. Leveraging safe lists as well as the list of hackers discovered by IDSs, the Ethereum protocol's smart contracts were upgraded in this stage. In the second stage, inter-blockchain operations were securely executed via encryption and cross-blockchain communication.

Mohammad Hossein Chinaei [10] have presented a decentralized, on-demand approach for verifying medical Internet of Things information. The following framework explains why and how to interface with smart contracts on a blockchain: Local witness equipment can commercialize their assertions without jeopardizing their confidentiality. Medical authorities can demand witness accounts for integrity checks of targeted sensors; local witness equipment can commercialize their remarks without jeopardizing their confidentiality. The authors created an optimization approach for medical authorities to choose the best group of accessible witnesses to obtain the highest validation likelihood while staying within a limit. The authors used real data from Wireless connections in a multi-story main campus to replicate the algorithm and demonstrate that a high verification likelihood may be obtained at a low cost of witnessing provision. This study is the first step enabling on-demand sensor network information witnessing that can be used in real-world circumstances.

Wassim Jerbi [11] Security issues, according to the author, are significantly limiting the progress and quick adoption of this sophisticated tech. Furthermore, the latter are unable to employ current security protocols and techniques since the majority of them do not guarantee reasonable performance or are not matched to the capabilities of devices, which are typically constrained in terms of data storage, computing, and power. Following a research, we discovered that our Block MDC protocol delivers all essential security services of the highest efficiency, as well as considerably more versatility and efficiency and time optimization for limited entities. The CHs have a comprehensive view of the cluster's components. The usage of blockchains allows for a dependable, decentralized, and tamper-proof log recording mechanism, as well as network activities.

III PROPOSED SYSTEM

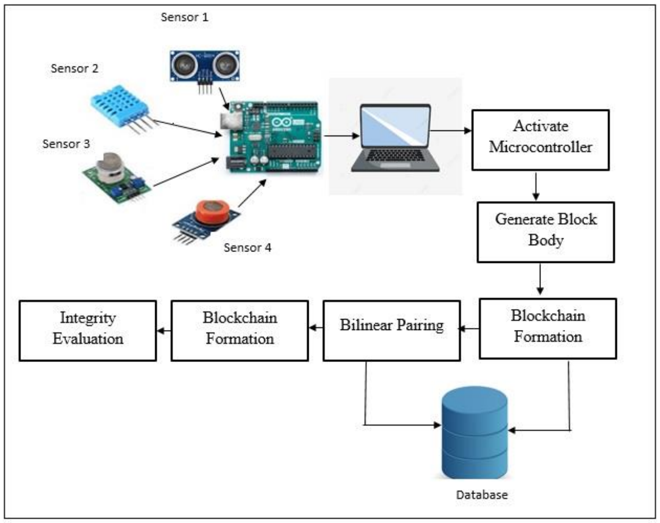


Figure 1: System Overview

The proposed approach for safeguarding the Internet of Things Data through the blockchain framework is represented in Figure 1 above, and the procedures taken to implement it are described below.

Step 1: *Sensor Data Collection* – For the purpose of initiating the approach the Arduino UNO microcontroller is interfaced with the development laptop. The Arduino UNO controller is being used for the purpose of connecting the sensors and collecting their readings. This setup includes the use of a number of different sensors, such as, ultrasonic, MQ5 gas sensor and an ambient temperature sensor. These sensors are connected to the microcontroller board and a sketch for collection and streaming of the sensor readings to the laptop.

The java code is initiated for the collection of the sensor data from the microcontroller. For this purpose an interactive graphical user interface has been created for the purpose of activating the sensor data collection engine. Once activated, a thread is initiated which listens on the COM27 port for the sensor values to be streamed. The sensor readings from the ultrasonic sensor, MQ5 gas sensor and the ambient temperature sensor are collected by the thread and then stored in the database along with the serial number and the current date and time. This will continue indefinitely as long as the thread is activated. The user interface provides the facility to stop the collection of the sensor values using a stop button provided specifically for this purpose that halts the running of the thread immediately.

Step 2: Blockchain formation – The blockchain framework is being utilized in this approach to facilitate the tamperproof protection to the sensor data. Once the data from the sensors is collected into the database and the thread collecting the data is halted, the blockchain can be created. The user interface provides the option to create the blockchain with the rows of the database containing the sensor values.

Once the user selects the operation for the blockchain creation, the system for the blockchain creation is initiated. The system then reads the database and extracts the values of the s no, ultrasonic sensor, MQ5 sensor and the temperature sensor, and the date and time. These values are then concatenated into a single string before being provided to the MD5 hashing mechanism. The MD5 hashing algorithm creates a 32 character hash key for the particular row’s concatenated values.

For the first initialization of this process, an empty string of the name terminal key is created. The resultant hash key of the first row is assigned to the terminal key and the system iterates to the next row of the database containing the sensor values. The entire process is repeated for the next row and the concatenated string is combined with the terminal key which is sent to the MD5 hashing approach to determine the 32 character hash key. The resultant hash key is then stored as a terminal key. This process is repeated for the rest of the rows of the database until the terminal key for the last row is obtained which is stored in the database for use in the next steps for the purpose of achieving the integrity evaluation.

The procedure of forming a blockchain for the stored sensor values in the database is depicted in algorithm 1 below.

ALGORITHM 1: Blockchain Formation

```
//Input : Sensor Values $S_V$
//Output: Terminal Key $T_K$
blockchainFormation($S_V$)
Start
$P_K$ =” ” [Previous Key]
for i=0 to size of $S_V$
    $C_S = \sum(A_{Ti})$
    $C_S = C_S + P_k$
    $T_K = MD5(C_S)$
end for
return $T_K$
Stop
```

Step 3: Integrity Evaluation through Bilinear Pairing– This phase makes use of the stored sensor values from the database table. The hash is generated using the MD5 hashing technique generating a 32 character hash key from the database rows. This entire procedure detailed in the previous step is performed again for the sensor data being stored in the database. This results in a terminal key that will be utilized for the purpose of achieving the integrity evaluation.

The terminal key is being used for the purpose of achieving the integrity evaluation through bilinear pairing. The bilinear pairing approach is a technique through with pairs of hash keys are compared for any presence of an avalanche effect in the keys. The process of hash key formation using MD5 hashing algorithm is very sensitive to the particular content being provided, any minute modification in the content could lead to a massive change in the resultant hash key. This is a main feature of the hashing approach that is being used to determine the integrity of the sensor values stored in the database.

To perform the integrity evaluation, these two pairs of terminal keys, the one generated in this step and the other generated previously and stored in the database are compared with one another. If there is any indication of the avalanche effect, then the database is tampered and a suitable alert is generated. If the keys are matching then the database is intact and there is no tampering being done on the database which indicates that the sensor values stored are secure.

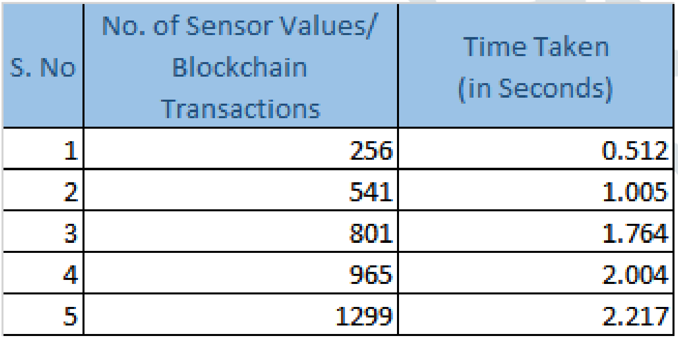
IV RESULT AND DISCUSSIONS

The proposed approach was developed using the Java programming language and the NetBeans IDE to safeguard IoT storage space using Blockchain. The development laptop has a Microsoft operating system, 6 GB ram, and 1 TB of storage capacity. Database administration is handled using the MySQL database.

The feasibility of the recommended technique has been rigorously assessed across a wide variety of parameters. The findings of the empirical investigation are presented below.

Scalability Analysis of Blockchain Transaction

The technique for securing IoT Information and maintaining its integrity through the framework of Blockchain is used to assess the scalability of Blockchain systems. For this objective, substantial examination is being conducted, including the creation of an interactive graphical interface for Internet of Things information acquisition and blockchain generation. The amount of Blockchain transactions which had already successfully documented and presented as seen in Table 1 below.



S. No	No. of Sensor Values/ Blockchain Transactions	Time Taken (in Seconds)
1	256	0.512
2	541	1.005
3	801	1.764
4	965	2.004
5	1299	2.217

Table 1: Blockchain Transaction Time Estimation Table

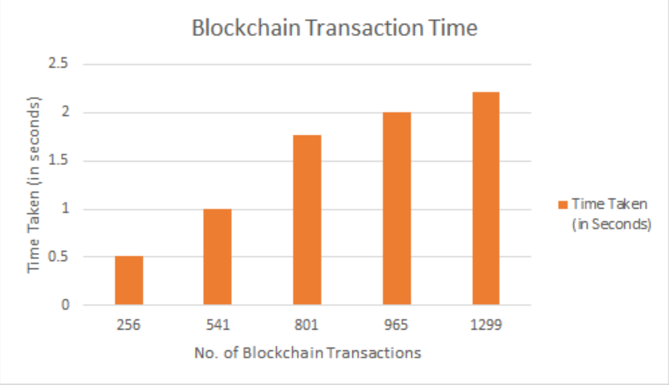


Figure 2: Blockchain Transactions

The graph shown in Figure 2 is created using the tabulated outcomes. The graphical representation has proven to be effective in demonstrating the relationship between the number of transactions and the time it takes to perform them on the Blockchain platform. The research' findings provide a deeper understanding of the methodological approach and the application of the Blockchain architecture to protect the privacy of IoT data. The number of IoT sensors or Blockchain processes is clearly not proportional to the time it requires to accomplish the process. This demonstrates that the Blockchain concept was applied successfully. The conclusions were helpful in understanding why the preserved IoT data was more secure.

V. CONCLUSION AND FUTURESCOPE

The IoT approach is necessary since this connects the information headroom constituted of information gathered from various sensing devices with the sensory environment comprises of different specialized items symbolized by sensors, breaks the spatial boundary among both subjects, and tends to make more timely and efficient evaluations through the interpretation of a variety of information, the Internet of Things (IoT) can introduce about improvements in a variety of disciplines. To collect IoT data, more IoT devices must be accessed in order to acquire additional information about the physical realm from various perspectives. The information obtained by these devices is particularly susceptible to manipulation or tampering. This is because the computational force and power available to these equipment are minimal. As a consequence, a simple and efficient method for enhancing the safety and confidentiality of data collected by Internet of Things sensors is necessary. This research approach has elaborated an effective approach through the use of the Blockchain framework for the purpose of achieving an effective security of the IoT data. The approach has been quantified for the time taken for the blockchain transactions which has been nominal.

The future research direction can utilize the IoT data which can be stored in the blockchain format on the cloud storage for improving the security further.

REFERENCES

[1] I. A. A. E. -M. And and S. M. Darwish, "Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach," in IEEE Access, vol. 9, pp. 103822-103834, 2021, doi: 10.1109/ACCESS.2021.3098933.

[2] S. Mori, "A Fundamental Analysis of Caching Data Protection Scheme using Light-weight Blockchain and Hashchain for Information-centric WSNs," 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2020, pp. 200-201, doi: 10.1109/BRAINS49436.2020.9223279.

[3] R. Wang, W. -T. Tsai, J. He, C. Liu, Q. Li and E. Deng, "A Video Surveillance System Based on Permissioned Blockchains and Edge Computing," 2019 IEEE International Conference on Big Data and Smart Computing (BigComp), 2019, pp. 1-6, doi: 10.1109/BIGCOMP.2019.8679354.

[4] G. Dittmann and J. Jelitto, "A Blockchain Proxy for Lightweight IoT Devices," 2019 Crypto Valley Conference on Blockchain Technology (CVCBT), 2019, pp. 82-85, doi: 10.1109/CVCBT.2019.00015.

[5] S. -J. Hsiao and W. -T. Sung, "Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks," in IEEE Access, vol. 9, pp. 72326-72341, 2021, doi: 10.1109/ACCESS.2021.3079708.

[6] A. Primo, "A Comparison of Blockchain-Based Wireless Sensor Network Protocols," 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2020, pp. 0793-0799, doi: 10.1109/UEMCON51285.2020.9298055.

[7] A. D. Wissner-Gross, J. C. Willard and N. Weston, "Tamper-Proofing Imagery from Distributed Sensors Using Learned Blockchain Consensus," 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), 2020, pp. 1-4, doi: 10.1109/AIPR50011.2020.9425050.

[8] S. Malik, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains," 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 184-193, doi: 10.1109/Blockchain.2019.00032.

[9] M. H. Salih Mohammed, "A Hybrid Framework for Securing Data Transmission in Internet of Things (IoTs) Environment using Blockchain Approach," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-10, doi: 10.1109/IEMTRONICS52119.2021.9422587.

[10] M. H. Chinaei, H. Habibi Gharakheili and V. Sivaraman, "Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract," in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 10117-10130, 15 June15, 2021, doi: 10.1109/JIOT.2021.3051433.

[11] W. Jerbi, O. Cheikhrouhou, A. Guermazi, H. Hamam and H. Trabelsi, "A Blockchain based Authentication Scheme for Mobile Data Collector in IoT," 2021 International Wireless Communications and Mobile Computing (IWCMC), 2021, pp. 929-934, doi: 10.1109/IWCMC51323.2021.9498656..