IJBPAS, November, Special Issue, 2021, 10(11): 551-562

ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)

'A Bridge Between Laboratory and Reader'

www.ijbpas.com

IOT SUSTAINABLE INTEGRITY SYSTEM SERVICES FOR SECURITY ENVIRONMENT DATA MANAGEMENT BASED ON BLOCKCHAIN

KAMALESHWAR.T[1*], RUCHI MEHROTRA JOSHI[2], FAROOQ SUNAR MAHAMMAD[3], SRIDEVI.R[4], PRATEEM PAN[5] AND JAMBERI.K[6]

1: Assistant Professor in Computer Science and Engineering at Veltech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi, Chennai, India

2: Associate Professor in University of Petroleum and Energy Studies, Dehradun, India

3: Associate Professor in Computer Science and Engineering at Santhiram Engineering College, Nandyal, Andhra Pradesh, India

4: Professor in Computer Science and Engineering at K.Ramakrishnan College of Engineering, Samayapuram, Trichy Tamil Nadu, India

5: Research Scholar in Electrical Engineering at National Institute of Technology Patna, Patna, Bihar, India

6: Assistant Professor in Computer science at S.A. College of arts & Science, Veeraraghavapuram, Chennai-77

***Corresponding Author: Kamaleshwar.T; E Mail: drtkamaleshwar@veltech.edu.in**

Received 20th July 2021; Revised 22nd Aug. 2021; Accepted 30th Sept. 2021; Available online 1st Nov. 2021

https://doi.org/10.31032/IJBPAS/2021/10.11.1048

ABSTRACT

The cutting-edge centralized Internet of Things (IoT) information flow pipeline is beginning to show its age as it struggles to keep up with the growing amount of individuals linked to IoT systems. As an outcome, the community is starting to move toward a decentralized pipeline to foster information & sharing of resources. The transition, although, isn't simple. How could they guarantee the accuracy of IoT information or processes provided by third parties when several instances allocate information/services randomly? Additionally, how might IoT information assist in deciding which side is responsible for improper behavior in the event of disputes? Lastly, as the amount of sharing grows, so does the amount of Service Level Agreements. The issue becomes how to get a natural Service Level Agreements creation and verification procedure that can be automated rather than going thru a laborious and time-consuming legalizing method with a trusted person. In this work, we investigate blockchain solutions to these problems & offer data integrity capabilities for IoT big data administration. They propose 5 integrity protocols for 3 parts of IoT processes: information transmission (data transit), data storage (data as rest), & data analysis (data processing). The procedure is then designed using selected articles of the survey as construction blocks. They increase the overall utility of IoT data & instructions produced in the Internet-of-things system by making them tamper-proof, traceable, non-repudiable, and much more robust utilizing the approach.

Keywords*:* Blockchain; IoT; Big data management; Service Level Agreement; Secure Environment

INTRODUCTION

Developers have been using centralized IoT architectures for years, ever since Kevin Ashton invented the phrase. This method is still used by several cutting-edge IoT devices, like Philips Hue & Amazon **[1]**. Such centralization is due to several variables. To begin with, the economy of IoT pushes IoT gadgets to become constricted gadgets to encourage widespread adoption. The corporation then constructs centralized remote servers that collect IoT information and perform the calculations that those gadgets need **[2]**. The server ultimately accumulates IoT information and gives improved IoT solutions, which may be valued further in the long term than the industry's earlier hardware expenditure in those IoT gadgets. Besides, in a centralized design, managing IoT massive data is simple. In terms of safety, administrators only have to protect the servers wherein IoT information is stored, and they often overlook the safety of IoT. They could also utilize Application Programming Interfaces to share information with other entities **[3]**. It is convenient because the corporation could conduct numerous things from one location (Cloud servers).

As IoT systems get more complex, centralized design suffers from a single point failure, low scaling, excessive latency, & privacy concerns. To address these difficulties, the IoT group is moving toward a decentralized design **[4]**. This shift, therefore, is difficult to materialize. Since multiple entities share information, actions, & services, the IoT flow of data has gotten increasingly sophisticated **[5]**. The IoT information flow pipeline becomes increasingly complex as an outcome of this sophistication, which increases information fragment. Bad management & unauthorized interference in one portion of the pipeline can cause inefficiencies or failure in certain IoT processes, resulting in financial loss **[6]**. To ensure the validity of the IoT activity in this new decentralized structure, they need a dependable environment that could track arbitrary IoT flow of data.

Related Works

The rising popularity of blockchain demonstrates significant potential for decentralization through its cryptocurrencies **[7]**. Several experts claim that blockchain could be applied to noncryptocurrency fields as well. For instance, in the IoT, blockchain could simplify information & resource sharing, provide a marketplace of IoT objects, to permit automation in certain sections of IoT operations using verifiable properties **[8]**.

This work explores the blockchain that could provide sustained integrity services of IoT large data administration, in line with those authors' statements **[9]**. This talk focuses on the data integrity challenges within IoT information flow pipeline during 3 IoT operating stages: transmitted data (data on transit), data storage (data as rest), & processing time (data process). Begin by conducting a literature review of current blockchain constantly works to every one of the stages, and they discover various blockchain-based techniques. Their recommended solutions, on either hand, address specific difficulties **[10]**. However, they contend that decentralized IoT activities are mutually dependent **[11]**. As a result, a grand architecture is necessary to guarantee that the integrity of the system is maintained during those stages.

The core IoT information from a single system tells us very little, such as the actual temperature in the neighborhood. It could be beneficial to some level; but, if they have more information or integrate with other IoT, it will be more enticing. E.g., they may calculate the elevated/low temps for a day (24hrs, from 12 AM -12 PM) by collecting the sensor's temp readings regularly (e.g., every 10 minutes). If they track & keep temp data for decades, they can also detect possible greenhouse effects **[12]**. Furthermore, scattering more temperature sensors among multiple neighborhoods provides us with other valuable insights, including establishing the average temp for entire neighborhoods or the warmest or coolest places.

However, the majority of IoT devices were machines with limited resources. As a result, they are unable to handle information from the IoT on their own. The most cutting-edge IoT information processing takes place on strong servers located far outside the devices. This place is frequently referred to as Cloud **[13]**.

IoT gadgets, such as sensors & actuators, make up the sensor. Sensors produce IoT information, & actuators await instructions via IoT applications. IoT bridges sit among IoT devices & applications at the middleware, intercepting IoT information and performing micro-processing. Information could be a data cleaning procedure, in which the portal removes duplication or erroneous data for providing that to IoT applications, or aggregation of data, in which the portal combines comparable data **[14]** as one IoT set of data. IoT solutions inside the application level are used to collect & aggregated serve IoT data to customers. IoT employees operate in the layer of processing to educate IoT information utilizing machine learning techniques to acquire insights. Employees deliver educated analytical outcomes back to IoT services, which the solutions might subsequently pass on to users of the application as feedback **[15]**. Moreover, the network layer manages data transmission among IoT objects. They could employ a variety of channels among gadgets & gateways, including Bluetooth, Zigbee, & 6Low-PAN. However, they can send information from gateways into applications, assistance to employees, & vice-versa, utilizing well-known Transmission Control Protocol/Internet Protocol stacks.

They had 3 kinds of IoT activities running across those described earlier tiers. To begin, information in transit refers to the steps they take when transmitting data from the IoT. Those stages are typically carried out at the network layer, wherein entities exchange IoT information. Secondly, information at rest refers to the process for storing IoT location data in the database. During actual-time application utilize cases, a middleware layer might temporarily save IoT information. Once this information is no longer required, they may remove it. However, for analytical & display reasons, the presentation layer retains IoT information in a database indefinitely **[16]**. This layer can store a large amount of data, which is frequently distributed over multiple servers.

Third, they put the data from the IoT into a phase they call data in progress. Micro & macro processings within middleware & processing levels are examples of these processes.

METHODOLOGY

They commonly build secure communication, a transmitting channel that provides various security assurances, to preserve the integrity of sent IoT information over the Internet. To begin with, this channel ensures that users are talking with legitimate entities rather than imposters. Second, the given data is only visible to those who are engaged. Others should never be able to learn anything about the data being communicated. Finally, the participants have confidence that the information they get is authentic, and that no third parties have tampered with this. To create a secure route, they could leverage existing encrypt & digital signature systems. Yet, they discovered that secure station's fundamental components, primarily identity service providers among organizations in the IoT flow of data pipeline, are not safe.

A centralized Certificate Authority serves as a third party in the PKI infrastructure. Other parties could trust Certificate Authority by allowing them to verify their public key. Outsiders who could show that the Certificate Authority signed a public key must see that it belongs to a legitimate entity because the Certificate Authority has already validated it. To put it another way, they recognize & believe any public key signed by the Certificate Authority. Similar flaws can also be found in the DNS. The DNS service, which is widely utilized, organizes and centralizes the mapping among domain names & Internet Protocol addresses. DNS servers, particularly DNS root datacenters, thus had complete control over the registered identities. By using DNS design, they encounter the same issues that they did with the PKI setup.

To their knowledge, no thorough design exists that demonstrates how such decentralized identities might be utilized to create a safe route. To close that gap, we use blockchain to build both decentralized authentication mechanisms & secure route creation. They do a literature review on various blockchain-related information in transit systems while mapping their concept. The picked papers from their survey are then used as the foundation for their layout.

During IoT data gathering, they could use solutions with their data in transit architecture to maintain the sanctity of transmitted IoT information over a secure connection. Therefore, because it simply protects communication, this security is transitory. It is typical for IoT entities that transmit IoT information or processes in the IoT platform. When a specific entity receives information from others, it decodes it, saves it, & proceeds to process it in plain text. Eventually, the entity would construct another safe route to transfer the processed information to some other entity. Since their information in transit only meets the integrity among entities who establish the secure connection, if attackers could compromise a few of those IoT firms, the IoT information loses its total validity. These entities were unable to assess communication quality since they were not participating in it. As a result, we believe that greater security in the IoT information itself is required to assure continuing integrity function.

Proposed work

These explanations are split into 2 parts: decentralized identity management & safe route creation. They're all part of IoT's total data integrity in transit. Every IoT entity will be able to recognize & authenticate each other thanks to their decentralized access control architecture. This identity system would be used all through the rest of our suggestions. Their architecture is depicted in **Figure 1**.

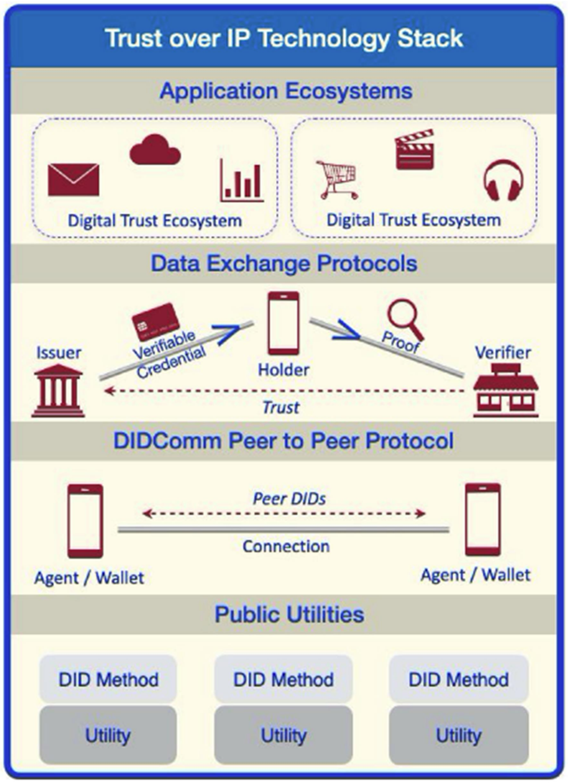

Figure 1: High-level decentralized authentication scheme

A betting concept is based on **[17]**, which proposes that users define the sum of money they were ready to risk to confirm a specific public key. The mechanism modifies the amount of trust by taking into account the number of contributions, with such a bigger wager equaling a greater trust. Furthermore, the algorithm considers the starting bet to calculate the reward that brand ambassadors can accept. Likewise, when the wager grows larger, the penalty (inside the form of lost reputation) grows as well.

This description shows how they might utilize our described earlier decentralized authentication mechanism to provide a safe conduit among IoT objects. The diagram of their secure communication concept is shown in **Figure 2**.

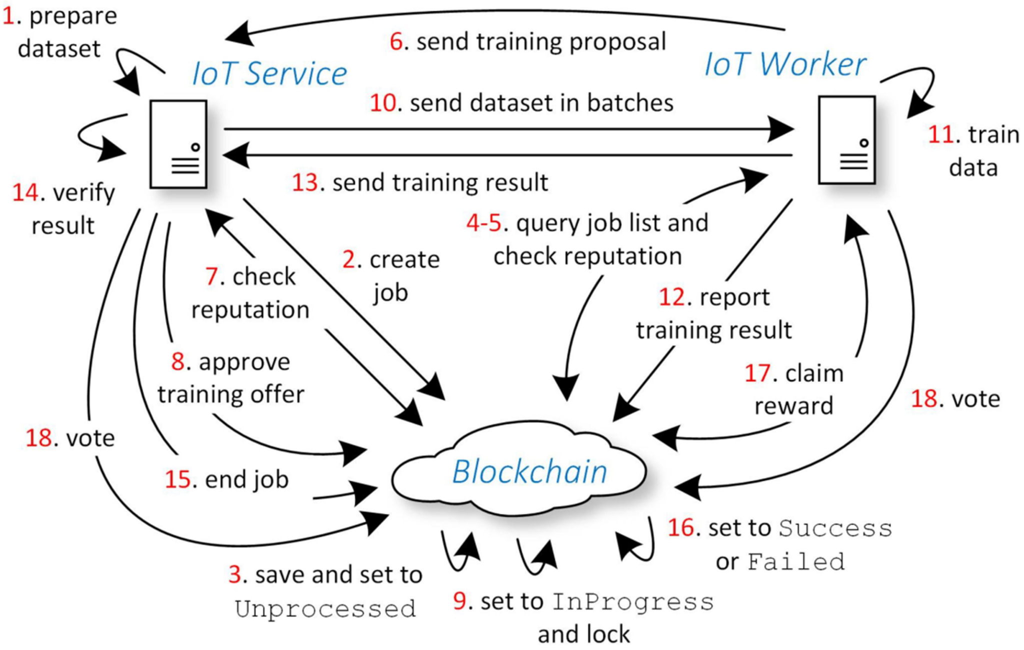
1. prepare dataset
IoT Service
6. send training proposal
IoT Worker
10. send dataset in batches
11. train data
13. send training result
14. verify result
4-5. query job list and check reputation
2. create job
7. check reputation
12. report training result
8. approve training offer
17. claim reward
18. vote
18. vote
15. end job
Blockchain
16. set to Success or Failed
3. save and set to Unprocessed
9. set to InProgress and lock

Figure 2: An overview of their TLS / DTLS secure communication architecture based on blockchain

The usage of a reputation process, as suggested in BATM, is something they support. 5 reputation components are defined by the researchers, which contain both positively and negatively incidents. By dividing the equation with a continually decreasing variable, their method additionally incorporates the freshness of episodes. The rating is the reputation rating that should be assigned. The services could only participate once during an amount of time, and it could vote either negatively or positively. The service delivers a favorable rating if all of the verifications are accurate. Instead, a negative value is assigned. They believe that as long as the majority of IoT services were trustworthy, they could retain a reputable certified reputation.

To dissuade malevolent actors from votes of spamming to a specific gateway by generating several fake profiles & providing dis-honest evaluations, they could impose a tiny payments system in transaction costs/deposits. Furthermore, the service publishes its customer & server-random as confirmation of a secure communication formation while casting a ballot. The given evidence would be audited by a notary as a trusted third-party observer. Any fraudulent report will be punished either by the system, which will prevent the malicious registrant from reclaiming their investment.

IoT objects submit their identification to the contract of smart, which is dispersed over numerous nodes in a network, utilizing our approach. As an outcome, their idea removes the system's one point of failure while increasing overall efficiency & scalability. Identification lookups became local processes because supplied public keys & domain addresses were duplicated to every blockchain node's store. Because the revoking list was likewise replicated to everyone nodes, this improvement accelerates the revoking process. Lastly, the lookups become secret because they are now local processes, which means no one else could log or filter their request of DNS query.

Both offline & online identification, each entity has a secret key, public key, & address. They also introduce a new entity, an auditor, who serves as a verifier for the information stored inside the IoT. An IoT system's blockchain units were all qualified into becoming auditors. An outline of their proposed data at rest architecture is shown in **Figure 3**. Their explanations are divided into three categories: IoT data gathering, IoT storage systems, & IoT information sharing. They also contribute to a database's overall integrity for recorded IoT information.

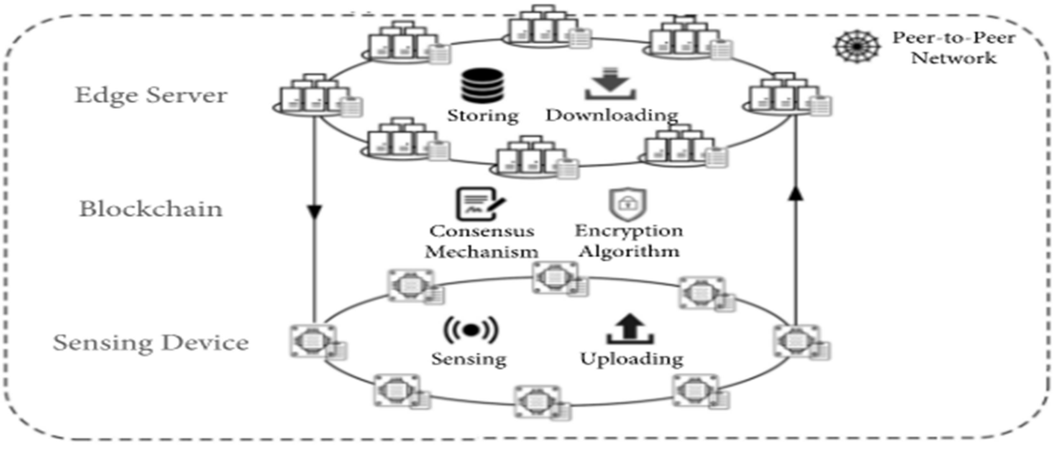

Figure 3: The integrity of stored IoT data is safeguarded

The IoT service gathers IoT basic data from numerous IoT devices throughout IoT activities. The information might be sent through one or more IoT gateway of micro-processing or even as a connection step to a service. As a result, the resulting IoT information could come from a variety of sources. Using a chain of signature, those affected parties sign the information they received before passing it on to others. They could track which entities were acquired, processed, & relayed when it concludes the communication pipeline. **Figure 4** shows their idea for a chain of signatures that may be utilized inside an IoT network, which they could further define as follows.

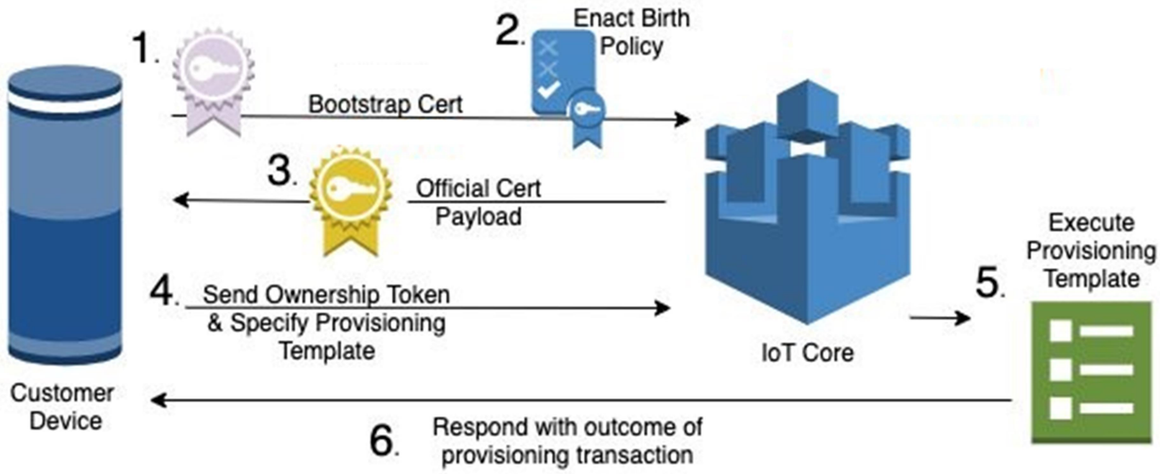
1.
Bootstrap Cert
2.
Enact Birth Policy
3.
Official Cert Payload
4.
Send Ownership Token & Specify Provisioning Template
5.
Execute Provisioning Template
6.
Respond with outcome of provisioning transaction
Customer Device
IoT Core

Figure 4: Four IoT flow of data situations employing chain signatures

When they save information in the blockchain, it produces transaction (tx) hashes. Since the blockchain is tamper-proof, such tx hashes represent invoices/evidence that specific data is available in blockchain, ensuring the data's legitimacy. These so-called "blockchain receipts" can be used to create a verified database. In most circumstances, the IoT service must distribute its recorded commands & data with other organizations for analysis or displays. The next sections describe how the second party, acting as an audit, might utilize blockchain invoices to verify randomly supplied information and calculate whether it's been tampered with.

Attackers had access to multiple compromised IoT devices in their situation. Next, to confuse/misidentify IoT devices, they generate phony/misleading inputs of the systems. The IoT management might have difficulty recognizing the source of assaults without non-repudiable & tamper-proof storage. They might assume that intrusion occurs at the IoT service, and this is where the information from the IoT is saved. They could even conjecture that the IoT gateway is transmitting erroneous data on the spur of the moment. Their approach adds non-repudiable and tamper-proof features to IoT databases. As a result, they could accelerate the detecting process. The system's records could be rapidly verified as safe, as well as the management could quickly assess whether the IoT devices themselves were hostile.

An entity in this system could become evil, whether purposefully or unintentionally, through partnerships among 2 parties. Let's imagine the first side violates the agreed-upon SLA via sending the second party fraudulent/invalid data. As a result, their actions cause harm to the recipient. By presenting the record of IoT information & directives to the court as proof, the second party could sue a first. Without the need for a non-repudiable & tamper-proof database, therefore, the supplied proof would lose its "sound of forensically" status & lack credibility. In comparison, they could retain the log's integrity & ensure its trust-worthiness using the mix of a chain of signatures & blockchain invoices which they suggest.

CONCLUSIONS

In 3 IoT stages: information in transit, information at rest, & information in the process, they suggested a grand architecture of blockchain-based ongoing integrity solution for IoT massive information management. To establish their architecture, they first articulated their objectives at every level & examined relevant blockchain studies from the literature as construction blocks. Following that, they presented their solutions. They suggested a decentralized authentication mechanism & secure route establishment blockchain based on data in transit. To improve the integrity of saved IoT information, they discussed the usage of a chain of identities linked using blockchain invoices. They then created a decentralized marketplace blockchain-based & learning federated allowing IoT objects to interact during the data collection process. Prospective adopters could try to incorporate their idea into their IoT systems in future developments. They claim that because the building elements were already in place, their approach must be possible to implement. More crucially, the key study directions should be a more in-depth examination of reputation & incentive mechanisms. These two factors, they suggest, were at the heart of decentralization since they could compel participants to follow the majority norm.

REFERENCES

[1] Wang H, Zhang J. Blockchain-based data integrity verification for largescale IoT data. IEEE Access. 2019 Nov 11; 7: 164996-5006.

[2] Zhao Q, Chen S, Liu Z, Baker T, Zhang Y. Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. Information Processing & Management. 2020 Nov 1; 57(6): 102355.

[3] Jamil F, Hang L, Kim K, Kim D. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. Electronics. 2019 May; 8(5): 505.

[4] Tian H, He J, Ding Y. Medical data management on the blockchain with privacy. Journal of medical systems. 2019 Feb; 43(2): 1-6.

[5] Garikapati, P., Balamurugan, K., Latchoumi, T. P., & Malkapuram, R. (2021). A Cluster-Profile Comparative Study on Machining AlSi 7/63% of SiC Hybrid Composite Using Agglomerative Hierarchical Clustering and K-Means. *Silicon*, 13, 961-972.

[6] Wei P, Wang D, Zhao Y, Tyagi SK, Kumar N. Blockchain data-based cloud data integrity protection mechanism. Future Generation Computer Systems. 2020 Jan 1; 102: 902-11.

[7] Ayoade G, Karande V, Khan L, Hamlen K. Decentralized IoT data management using blockchain and trusted execution environment. In2018 IEEE International Conference on Information Reuse and Integration (IRI) 2018 Jul 6 (pp. 15-22). IEEE.

[8] Hang L, Kim DH. Design and implementation of an integrated IoT blockchain platform for sensing data integrity. Sensors. 2019 Jan; 19(10): 2228.

[9] Liu B, Yu XL, Chen S, Xu X, Zhu L. Blockchain-based data integrity service framework for IoT data. In2017 IEEE International Conference on Web Services (ICWS) 2017 Jun 25 (pp. 468-475). IEEE.

[10] Jamil F, Ahmad S, Iqbal N, Kim DH. Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. Sensors. 2020 Jan; 20(8): 2195.

[11] Yang HK, Cha HJ, Song YJ. Secure identifier management based on Blockchain technology in the NDN environment. IEEE Access. 2018 Dec 4; 7: 6262-8.

[12] Dai H, Young HP, Durant TJ, Gong G, Kang M, Krumholz HM, Schulz WL, Jiang L. TrialChain: A blockchain-based platform to validate data integrity in large, biomedical research studies. arXiv preprint arXiv:1807.03662. 2018 Jul 10.

[13] Dimitrov DV. Blockchain applications for healthcare data management. Healthcare informatics research. 2019 Jan 31; 25(1): 51-6.

[14] Hasegawa Y, Yamamoto H. Reliable IoT Data Management Platform Based on Real-World Cooperation Through Blockchain. IEEE Consumer Electronics Magazine. 2020 Jul 24; 10(1): 82-92.

[15] Jung MY, Jang JW. Data management and searching system and method to provide increased security for IoT platforms. In2017 International conference on information and communication technology convergence (ICTC) 2017 Oct 18 (pp. 873-878). IEEE.

[16] Zhang Y, Xu C, Lin X, Shen XS. Blockchain-based public integrity verification for cloud storage against procrastinating auditors. IEEE Transactions on Cloud Computing. 2019 Mar 29.

[17] Hjálmarsson FÞ, Hreiðarsson GK, Hamdaqa M, Hjálmtýsson G. Blockchain-based e-voting system. In2018 IEEE 11th International Conference on Cloud Computing (CLOUD) 2018 Jul 2 (pp. 983-986). IEEE.