Implementing Adaptive Blockchain and Federated Analytics for Secure Cloud-Edge IoT Data Validation

D. Mahaboob Basha[1], G. Penchalaiah Babu[2], N. Rajini Kiranmai[3], A. Viswanatha Rao[4]

[1, 2, 3, 4]Assistant Professor in Computer Science and Applications, Department of Computer Science, St. Joseph's Degree College, Sunkesula Road, Kurnool, Andhra Pradesh
Corresponding Author Email: *bashad959[at]gmail.com*

Abstract: ***The proliferation of Internet of Things (IoT) devices has introduced an unprecedented level of connectivity, enabling seamless data exchange across various applications. However, this connectivity has also amplified security and privacy concerns, given the sensitivity of IoT-generated data. Integrating blockchain technology with edge and cloud computing frameworks offers a transformative solution for secure IoT data security. Blockchain ensures decentralized trust, data integrity, and immutability, while edge computing enhances real-time data processing and cloud computing provides scalable storage and processing capabilities. The design and implementation of cloud-based data integrity for IOT based blockchain platform framework describes the Data Integrity Service. This framework is more reliable and data integrity verification can be provided for both the Data Owners and the Data Consumers, without depending on any Third-Party Auditor (TPA). In this analysis, device management is important for organizations to maintain secure, up-to-date data and networks, protecting against unauthorized access. It includes tasks, data visualization, cloud interfaces, big data analytics, blockchain networks, and P2P protocol. The relevant protocols and a subsequent prototype system are implemented. Hence, this analysis shows better results in terms of accuracy, precision and efficiency.***

Keywords: Internet of Things, Blockchain, Data Integrity, Big Data Analytics, Data Visualization

1. Introduction

The Internet of Things (IoT) represents a transformative shift in the digital landscape, with interconnected devices forming a network that extends

Across industries such as healthcare, manufacturing, and smart cities [1]. While IoT enables significant advancements through continuous data collection and analysis, it also introduces vulnerabilities stemming from centralized data processing and storage systems. Traditional methods for securing IoT data often fail to scale efficiently or adapt to the dynamic nature of these networks. Similar to this, a lot of data is produced by the Internet of Things (IoT) [2], which connects people, devices, and objects. Organizations may find it difficult to control data because of different operating systems, different networking protocols, and application compatibility. However, it is advantageous to be able to get important information from the amount of data, these technologies release. Scalable processing and storage resources are provided by cloud computing technology, which can be utilized to help data management [3]. To fully realize the commercial opportunities in this industry, it takes platform-neutral solutions to solve fundamental issues including data interchange formats, security, interoperability, and communication bottlenecks [4].

Large-scale autonomous IoT systems are made possible by a combination of network and embedded computing technologies, which have developed together [5]. IoT systems are often made up of diverse devices that produce and distribute large amounts of privacy-sensitive and safety-critical data. The majority of IoT solutions available presently utilize a centralized architecture to establish Internet-based connections with cloud servers [6]. As IoT systems get more complicated, this approach offers improved computing and data management capabilities, but it still has a number of security issues. Because there are so many IoT devices, it is essential to create both a fault-tolerant network and a secured environment [7].

The numerous real-world applications, including medical record management, intelligent transportation systems, decentralized web applications, and prediction platforms, have already had high-level use cases developed [8]. In short, the key benefits of the blockchain are, its high efficiency, low cost, improved traceability, increased security, and lack of third-party attack [9].

The revolution in recording systems is blockchain technology, business and research communities have long predicted that it will be a major role in the monitoring, controlling, and, most crucially, security of Internet of Things devices [10]. The centralized architecture of today's networks presents privacy and security issues with IoT that the blockchain may be able to resolve, but there are still a number of scientific obstacles standing in the way of its incorporation [11].

In fact, most consensus methods used in modern blockchain systems weren't designed to run on devices with extremely limited processing capability. Numerous systems in use presently make use of Proof-of-work (PoW), the blockchain network's original consensus mechanism. It distributes decision-making authority among all of the different nodes, or miners. This procedure is known as mining that requires extremely high processing capabilities [12]. Compared to desktop systems, the development of embedded devices, such as smartphones, is occur more slowly [13]. Due to their low processing power and little data storage, these types of devices find it challenging to carry out transactions utilizing the present blockchain-based systems. Despite this, products with built-in blockchain capabilities are becoming more widely available. One example is EthEmbedded, which lets embedded devices run the full Ethereum node, including Raspberry Pi and Beaglebone Black [14]. Moreover, Raspnode supports the usage of wallets for Bitcoin and Litecoin, authorizing the use of embedded devices for mining. But as Raspnode pointed out, mining on IoT devices would be useless. On the other hand, some devices are designed for mining, including as Application-specific integrated circuit (ASIC) chips, need not to be utilized in connection with IoT devices. There is still a lot of study to be done before IoT devices can be widely integrated as blockchain components [15].

Blockchain technology has emerged as a promising candidate for addressing IoT security concerns. With its decentralized architecture and cryptographic protocols, blockchain ensures transparency, immutability, and trust among stakeholders. However, the high computational and energy demands of blockchain systems pose challenges for IoT devices, which often operate under resource constraints. Integrating blockchain with edge and cloud computing presents an innovative solution to this dilemma. Edge computing allows data processing closer to IoT devices, reducing latency and enhancing real-time decision-making. Cloud computing complements this by offering scalability and storage for aggregated data. Together, these technologies form a robust framework for secure IoT data exchange.

2. Literature Survey

H. Wang and J. Zhang, et al. [16] presented large-scale IoT data a Blockchain and Bilinear Mapping-based Data Integrity Scheme (BB-DIS), which creates homomorphic verifiable tags for sampling verification and divides data into parts. By using blockchain transactions and the properties of bilinear mapping, data integrity can be achieved. A thorough examination of the BB-DIS's performance analysis is also included, such as security, complexity, dynamicity, and feasibility. They, then demonstrate the verification scheme's implementation with a BB-DIS prototype system.

K. O. B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia and J. Gao, et al. [17] proposed secure data transfer method in cloud environments based on proxy re-encryption will receive encrypted data from data owners due to identity-based encryption, where it can be accessed by authorized users are using proxy re-encryption construction. The cloud can receive encrypted data from data owners due to identity-based encryption, where it can be accessed by authorized users are using proxy re-encryption construction. Because Internet of Things devices have limited resources, to handle highly computational operations, an edge device acts as a proxy server.

U. Demirbaga and G. S. Aujla, et al. [18] IoT systems supports in important decision-making to identity verification, data integrity, and privacy protection are crucial requirements for big data service management in the healthcare industry. This method uses blockchain technology and big data systems are securely store, analyze, and verified access to data from IoT-enabled devices. In addition to preventing data link capability, the zero-knowledge protocol makes sure that no information is available to unauthenticated users. The results show that the strategy works to address big data analytics and privacy concerns in the healthcare industry.

Y. Lin, J. Li, S. Kimura, Y. Yang, Y. Ji and Y. Cao, et al. [19] Consortium blockchain-based public integrity verification (CBPIV) is done through a mechanism In order for authorized parties to audit the auditor and verify that the verification results are accurate, the auditor actions in CBPIV are documented in the consortium (a group made up of two or more individuals, companies, or governments that work together to achieving a common objective) blockchain. The suggested approach is safe and minimizes the load on data owners with low computing capacity, according to the performance and security evaluations.

J. H. Khor, M. Sidorov, M. T. Ong and S. Y. Chua, et al. [20] data protection mechanism that could help lower transaction costs, maintain the data integrity of sensor data saved, and increase the battery life of Internet of Things (IoT) devices connected to public blockchain networks. An ESP32S2 device is used as a proof of concept to evaluate and verify the suggested data storage protocol's functionality. A formal smart contract analysis tool is used in the design and analysis of a smart contract. The sensor data that was taken from the public blockchain is intended to be shown and validated through a decentralized Web application.

Y. J. Chen, L. C. Wang and S. Wang, et al. [21] data integrity protection approach to the Internet of Things (IoT) based on blockchain technology. Due to their centralized architecture, traditional data integrity techniques like Public key infrastructure (PKI), network congestion and single points of failure are problems for symmetric key schemes. Motivated by blockchain's distributed data authentication, they suggest implementing blockchain technology to guarantee data integrity in IoT networks. IoT nodes with constrained computational and network resources, cannot be directly integrated into the current blockchain architecture. Lastly, they suggest a low-power mining procedure that limits the competition for block creation to IoT edge nodes only, allowing them to share the block with other nodes.

L. Hou, X. Xu, K. Zheng and X. Wang, et al. [22] combining RAFT (Reliable, Replicated, Redundant, And Fault-Tolerant) consensus with Multi-Access Edge Computing (MEC), effective and inaccessible edge data services for IoT applications can be obtained by implementing blockchain on reliable base stations and gateways. Reducing blockchain data storage latency is still difficult, although, when block formation speed in a given region increases by anomaly-driven data flow. In order to effectively move transactions from busy locations to idle regions in IoT applications, an intelligent transaction migration plan for private blockchains based on RAFT is proposed. The suggested strategy appears to be able to lower latency under conditions of heavy data flow, according to simulation results.

S. Dhaka, Y. J. Chen, S. De and L. C. Wang, et al. [23] innovative lightweight stochastic blockchain for wireless Internet of Things (IoT) devices are based on confidence scores. In order to make it easier to choose more reliable validator nodes and decrease the possibility of choosing malicious validators, the received signal strength is utilized to determine a wireless IoT node's trust level. Based on simulations and analysis, they find that the probability of effectively protecting against data integrity attacks (i.e., maintaining that most validator nodes remain unhacked) can be enhanced up to two times more than that of the closest competitive random selection scheme in stochastic blockchains. This result shows that the number of validator nodes and total nodes in the network is affect the probability of a successful defense. The suggested blockchain concept can be quickly put into practice in a number of wireless Internet of things to improve the system's ability to successfully defend IoT data integrity.

Y. Li, Z. Li, B. Yang and Y. Ding, et al. [24] verify data integrity for Cloud-IoT situations, suggest a public scheme called Data Integrity Verification scheme. The data auditing can be effectively completed by using an algebraic signature and homomorphic hash function. In order to better protect IoT users privacy and stop IoT data leaks, this also uses blind technology. In order to increase auditing effectiveness and satisfy realistic requires for Cloud-IoT scenarios, batch auditing is developed. Additionally, the Improved Divide & Conquer Table (ID&CT), a new data structure, was designed to achieve effective data dynamics. Finally, the performance and security analysis is more effective and secure.

Q. Zhang, et al. [25] enhancing the auditing process in decentralized storage networks with blockchain technology; yet, as audit requests increase, the on-chain overhead continues to grow linearly. Overloading blockchain networks is inevitable. This paper presents a data integrity auditing system that performs well in decentralized storage for numerous copies. Specifically, first, they provide a simple method for verifying several copies of a single file using various polynomial commitment techniques, and then, for multiple copies of numerous files, they suggest an efficient batch auditing approach. With a constant on-chain storage cost, this technique may significantly decrease the computing overhead of storage service providers. Performance and security analyses demonstrate the efficiency and usefulness of this approach.

3. Framework of Implementing Adaptive Blockchain and Federated Analytics for Secure Cloud-Edge IoT Data Validation

In this section, framework of Implementing Adaptive Blockchain and Federated Analytics For Secure Cloud-Edge IOT Data Validation is observed in figure 1. Device management is an essential element of every organization's security plan since it keeps data and networks that are secure, up-to-date and conform to business requirements while protecting against unauthorized access. Device management is classified into task management and data visualization integrated into generic Cloud interface to big data analytics to the blockchain network and it is spitted into Peer-To-Peer (P2P) protocol and event management. In this method, device management is important for organizations to maintain security, up-to-date data and networks and protecting against unauthorized access. Even data visualization, blockchain networks, cloud interfaces, big data analytics, tasks and P2P protocol.

Then, it is integrated to routing protocol, it is classified to control panel and load balancer. It is processing for computing resources and it is stored. The method of successfully and efficiently monitoring, managing, carrying out a task's or several tasks task management refers to managing a project's whole life cycle, from conception to conclusion. To make a task or project more effective, efficient, and helpful to communication is the goal of task management. Using popular images, data visualization is the process of presenting data with visual tools including plots, charts and even animations.

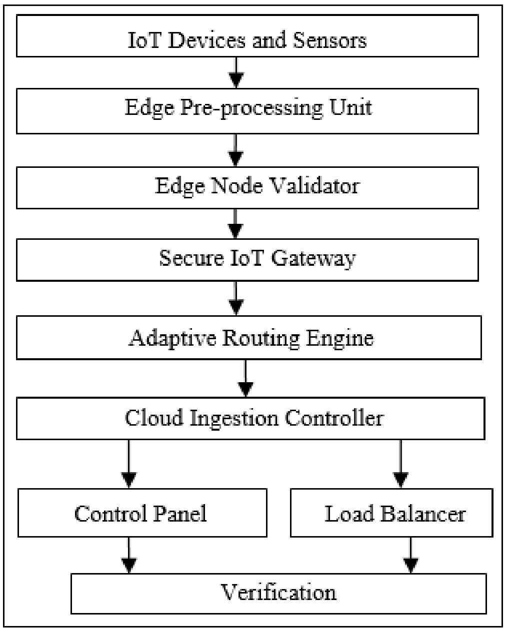

Figure 1: Framework of Implementing Adaptive Blockchain and Federated Analytics For Secure Cloud-Edge IOT Data Validation

Sensor servers, middleware, applications, and the Cloud platform are all mediated by the general Cloud interface, while complicated data connections and insights are communicated through visual displays. For alphanumeric and time series data from sensors and IoT devices, it offers an easy-to-use interface and supports a wide range of formats. Platform-neutral data transfer formats are used in different Cloud settings to improve interoperability. Making data-informed decisions can be supported by big data analytics, which is the process of identifying trends, patterns, and correlations in large amounts of raw data. With the support of more recent technologies, these procedures use well-known statistical analysis methods, such as regression and clustering, to larger datasets. A collection of computers connected through Peer-to-Peer (P2P) networking share the same permissions and responsibilities when it comes to data processing. The process of planning and organizing an event is called event management. The planning phase of this procedure starts at the beginning and ends with post-event development of strategies.

Route management is the strategic planning of routes for the delivery of services, products, or materials. Viewing and modifying system settings is possible with Microsoft

Windows Control Panel. All resource servers are used equally due to the work of a load balancer, it operates as an unseen facilitator and supports the user and server group. It works as a facilitator that is invisible. Compute resources are infrastructure components hardware or software that make it possible to receive, analyze, and store data in order to solve problems and create solutions. The process of storing digital data in a data storage device is involves the use of computing technology for storage. A computer may keep data for a certain amount of time or permanently through a technique called storage.

4. Result Analysis

In this section, performance analysis of Implementing Adaptive Blockchain and Federated Analytics for Secure Cloud-Edge IOT Data Validation is observed. Table.1, shows performance comparison between existing system and proposed system with the parameters interms of accuracy, precision and efficiency.

Table 1: Performance Analysis

Parameters	Existing System	Proposed System
Accuracy	91.5	96.8
Precision	82.1	88
Efficiency	86.7	88.4

In Figure 2, accuracy comparison graph is observed between the exisitng system and proposed system. Then the IOT-based block chain platform shows high accuracy for implementing Adaptive Blockchain and Federated Analytics for Secure Cloud-Edge IOT Data Validation.

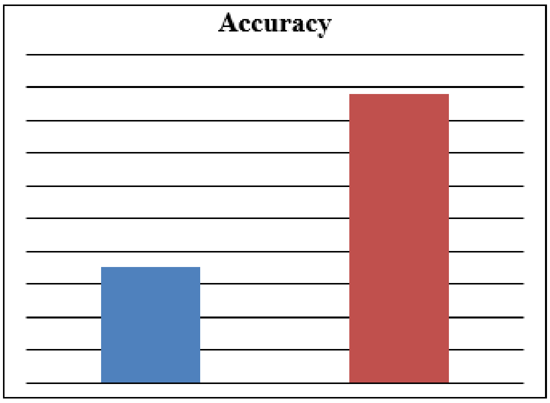

Figure 2: Accuracy Comparison Graph

The precision comparison graph between the existing system and proposed system is seen in Figure 3. A high precision is achieved in implementing Adaptive Blockchain and Federated Analytics for Secure Cloud-Edge IOT Data Validation.

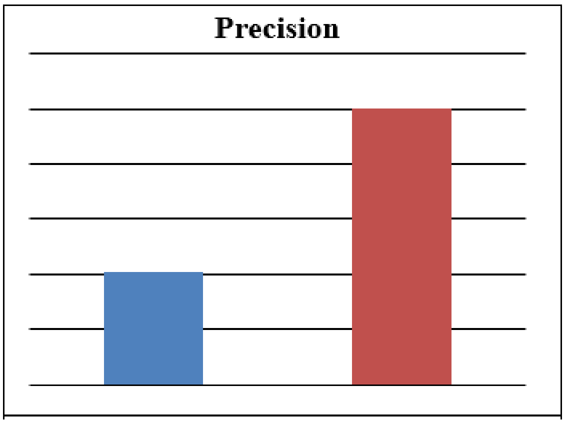

Figure 3: Precision Comparison Graph

In Figure 4, efficiency comparison graph is observed between the existing system and proposed system. Then the IOT-based block chain platform shows high efficiency for design and implementing Adaptive Blockchain and Federated Analytics for Secure Cloud-Edge IOT Data Validation.

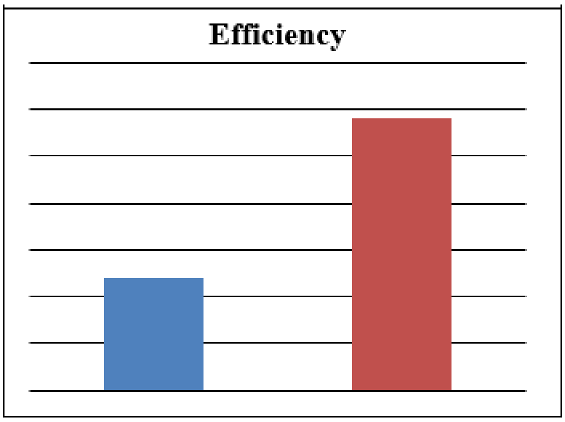

Figure 4: Efficiency Comparison Graph

5. Conclusion

In this section implementing Adaptive Blockchain and Federated Analytics for Secure Cloud-Edge IOT Data Validation is concluded. Blockchain technologies provided a new security protocol and infrastructure to enable billions of IoT devices to have trusted interoperability for both data owners and users. In traditional methods, precision and efficiency are not accurate. Therefore, this design and implementation of cloud-based data integrity for IOT based blockchain platform framework didn't depended on any Third Party Auditor (TPA) for Data Integrity Service and this device management is important for organizations to maintain the secured, up-to-date data and networks, protected against unauthorized access. Therefore, by using this system accuracy, precision and efficiency are better when compared with existing system. It includes tasks, data visualization, cloud interfaces, big data analytics, blockchain networks, and P2P protocol. In future, by using this system further parameters like security and storage cost will improve.

References

[1] A. A. Sadawi, M. S. Hassan and M. Ndiaye, "A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges," in IEEE

Access, vol. 9, pp. 54478-54497, 2021, doi: 10.1109/ACCESS.2021.3070555.

[2] S. Lee and J. -H. Kim, "Opportunistic Block Validation for IoT Blockchain Networks," in IEEE Internet of Things Journal, vol. 11, no. 1, pp. 666-676, 1 Jan.1, 2024, doi: 10.1109/JIOT.2023.3287166.

[3] A. P. Kalapaaking, I. Khalil, M. S. Rahman, M. Atiquzzaman, X. Yi and M. Almashor, "Blockchain-Based Federated Learning With Secure Aggregation in Trusted Execution Environment for Internet-of-Things," in IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1703-1714, Feb. 2023, doi: 10.1109/TII.2022.3170348.

[4] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges," in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2521 2549, Fourthquarter 2020, doi: 10.1109/COMST.2020.3020092.

[5] K. H. Alyoubi, A. O. Khadidos, A. M. Alshareef, D. Hamed, A. O. Khadidos and M. Ragab, "Capuchin Search Algorithm with Deep Learning-Based Data Edge Verification for Blockchain-Assisted IoT Environment," in IEEE Access, vol. 12, pp. 351-360, 2024, doi: 10.1109/ACCESS.2023.3346437.

[6] W. Lin., "Blockchain Technology in Current Agricultural Systems: From Techniques to Applications," in IEEE Access, vol. 8, pp. 143920-143937, 2020, doi: 10.1109/ACCESS.2020.3014522.

[7] A. Haddad, M. H. Habaebi, M. R. Islam, N. F. Hasbullah and S. A. Zabidi, "Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems," in IEEE Access, vol. 10, pp. 94583-94615, 2022, doi: 10.1109/ACCESS.2022.3201878.

[8] W. A. Mahrous, M. Farouk and S. M. Darwish, "An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash," in IEEE Access, vol. 9, pp. 151327-151336, 2021, doi: 10.1109/ACCESS.2021.3126715.

[9] H. Guo, W. Li and M. Nejad, "A Hierarchical and Location-Aware Consensus Protocol for IoT-Blockchain Applications," in IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2972-2986, Sept. 2022, doi: 10.1109/TNSM.2022.3176607.

[10] T. Ma, B. Du, M. Li, J. Li, Y. Shi and H. Fan, "Toward Data Authenticity and Integrity for Blockchain-Based Mobile Edge Computing," in IEEE Sensors Journal, vol. 22, no. 10, pp. 9967-9980, 15 May15, 2022, doi: 10.1109/JSEN.2022.3163915.

[11] Parmar, Martin & Shah, Parth. (2023). Internet of things-blockchain integration: a robust data security approach for end-to-end communication. Indonesian Journal of Electrical Engineering and Computer Science. vol. 32, no. 2, pp. 1050-1057. doi: 10.11591/ijeecs.v32.i2.pp1050-1057.

[12] Sodinapalli, Nagendra Prasad et al. “An efficient resource utilization technique for scheduling scientific workload in cloud computing environment.” IAES International Journal of Artificial Intelligence (IJ-AI) vol. 11, no. 1, March 2022, pp. 367-378 ISSN: 2252-8938, doi: 10.11591/ijai.v11.i1.pp367-378

[13] Jawhar, Muna.. Detecting network attacks model based on a convolutional neural network. International Journal of Electrical and Computer Engineering. vol. 13.no. 3, pp. 3072~3078. doi: 10.11591/ijece.v13i3.pp3072-3078.

[14] Z. Liu, L. Hou, K. Zheng, Q. Zhou and S. Mao, "A DQN-Based Consensus Mechanism for Blockchain in IoT Networks," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11962-11973, 15 July15, 2022, doi: 10.1109/JIOT.2021.3132420

[15] A. Rashid and A. U. R. Khan, "Blockchain-Based Autonomous Authentication and Integrity for Internet of Battlefield Things in C3I System," in IEEE Access, vol. 10, pp. 91572-91587, 2022, doi: 10.1109/ACCESS.2022.3201815

[16] H. Wang and J. Zhang, "Blockchain Based Data Integrity Verification for Large-Scale IoT Data," in IEEE Access, vol. 7, pp. 164996-165006, 2019, doi: 10.1109/ACCESS.2019.2952635.

[17] K. O. B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia and J. Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," in IEEE Systems Journal, vol. 16, no. 1, pp. 1685-1696, March 2022, doi: 10.1109/JSYST.2021.3076759.

[18] U. Demirbaga and G. S. Aujla, "MapChain: A Blockchain-Based Verifiable Healthcare Service Management in IoT-Based Big Data Ecosystem," in IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 3896-3907, Dec. 2022, doi: 10.1109/TNSM.2022.3204851

[19] Y. Lin, J. Li, S. Kimura, Y. Yang, Y. Ji and Y. Cao, "Consortium Blockchain-Based Public Integrity Verification in Cloud Storage for IoT," in IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3978-3987, 1 March1, 2022, doi: 10.1109/JIOT.2021.3102236.

[20] J. H. Khor, M. Sidorov, M. T. Ong and S. Y. Chua, "Public Blockchain-Based Data Integrity Verification for Low-Power IoT Devices," in IEEE Internet of Things Journal, vol. 10, no. 14, pp. 13056-13064, 15 July15, 2023, doi: 10.1109/JIOT.2023.3259975

[21] Y. J. Chen, L. C. Wang and S. Wang, "Stochastic Blockchain for IoT Data Integrity," in IEEE Transactions on Network Science and Engineering, vol. 7, no. 1, pp. 373-384, 1 Jan.-March 2020, doi: 10.1109/TNSE.2018.2887236.

[22] L. Hou, X. Xu, K. Zheng and X. Wang, "An Intelligent Transaction Migration Scheme for RAFT-Based Private Blockchain in Internet of Things Applications," in IEEE Communications Letters, vol. 25, no. 8, pp. 2753-2757, Aug. 2021, doi: 10.1109/LCOMM.2021.3079201.

[23] S. Dhaka, Y. J. Chen, S. De and L. C. Wang, "A Lightweight Stochastic Blockchain for IoT Data Integrity in Wireless Channels," in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 765-781, 2023, doi: 10.1109/OJVT.2023.3317640.

[24] Y. Li, Z. Li, B. Yang and Y. Ding, "Algebraic Signature-Based Public Data Integrity Batch Verification for Cloud-IoT," in IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 3184-3196, 1 July-Sept. 2023, doi: 10.1109/TCC.2023.3266593.

[25] Q. Zhang., "Efficient Blockchain-Based Data Integrity Auditing for Multi-Copy in Decentralized Storage," in

IEEE Transactions on Parallel and Distributed Systems, vol. 34, no. 12, pp. 3162-3173, Dec. 2023, doi: 10.1109/TPDS.2023.3323155.