**THE "INTERNET OF THINGS STORAGE OF INFORMATION ON BLOCKCHAIN TECHNOLOGY WITH SECURITY AND IDENTIFICATION**

*1Mohammad abdul shoaib , 2N B Shashidhar ,3Naseerhuddhin, 4Mohammad salman areeb,*5*DR.P.SRINIVAS RAO*

# *1,2,3,4bachelor Degree, Cse,* *Jayamukhi Institute Of Technological Sciences Narsampet, Warangal.*

5*DR.P.SRINIVAS RAO, Associate Professor, bachelor Degree, Cse, Jayamukhi Institute Of Technological Sciences Narsampet, Warangal.*

**ABSTRACT:**

The Internet of Things (IoTs) is made up of several sensing devices with a range of capabilities that may be used for a number of different purposes.

In such situations, it is relatively difficult to safeguard networks against unauthorised information access and effectively utilise storage due to low data handling capabilities, limited storage, and security considerations. Despite the fact that researchers provide several security solutions

and data storage, however only a few options are suitable for IoTs with WSNs. For the safe communication in IoTs powered by wireless sensor networks (WSNs), a blockchain-based decentralised architecture combined with authentication and privacy-preserving techniques is created. In a cloud computing environment, communication with sensor nodes and base stations is conducted through registration, certification, and revocation processes. Cluster chiefs provide the data gathered under this plan to the BS.

As a result, BS logs all the crucial information on the decentralised blockchain and sends vast amounts of data to clouds for storage.

By using BS, all rogue nodes' revoked certificates are removed from the blockchain. The suggested scheme's effectiveness is evaluated in terms of detection precision, certification latency, computational overheads, and communicational overheads. The superiority of the suggested method over the existing approaches is supported by the simulated results, comparative analysis, and security validation.

**INTRODUCTION:**

In the modern day, wireless interaction and processing of data are two areas where the Internet of Things (IoTs) is one of the most well-liked, practical, and dominant technologies [1]. The term "IoTs" refers to 'things' that can be identified, comprehended, managed, and found with the aid of the internet.

Due to the internet's communicational and computational capabilities, practically all IoT devices in use today may be connected to it, enabling the realisation of several additional and more suited applications [2]. In the Internet of Things, several sensor nodes are placed collaboratively for monitoring, sensing, and automating purposes. All of these nodes work together to build Wireless Sensor Networks (WSNs), which are integral to the Internet of Things (IoT) [3] and can sense and track any physical objects or activities that take place in a given area. The aforementioned sensor nodes, also referred to as "motes," are small, inexpensive, internally coupled, and dispersed in certain locations [4]. Because these sensor nodes integrate many sensing, processing, and communication capabilities over wireless media, physical events in WSNs may be tracked and detected in real time.

Although the deployment and operation of WSNs are application-specific in terms of the areas of interest, surveillance, sensing, broadcasting, and subsequent analysis of the gathered data are the main objectives [5]. [6].

But in the modern technological world, there is a great amount of information coming in at an astonishing velocity, and this needs to be dealt with. As is common knowledge, WSNs have a wide range of uses, including the military, business, smart homes, healthcare, surveillance, habitat monitoring, and agriculture, to mention a few. [7] [8]. The core of WSN, the sensor nodes, are constrained in terms of their energy, computing power, storage capacity, and communication bandwidth. Therefore, as the IoT increasingly raises the need for WSNs, new difficulties are being discovered for their effective implementation. Additionally, security is a major problem for WSN-enabled IoT.

The security of the network is put in jeopardy if an enemy assaults it and purposefully compromises the nodes. As a result, before participating actively in the IoT infrastructure, WSNs must identify and remove rogue nodes from the network.

**RELATED WORK:**

However, new literatures connected to WSNs-based IoT using the technology of blockchain are briefly examined for the data storage, registration, and security. This is done before addressing the suggested network model and findings gained. IoT devices generate a lot of data, which has to be efficiently stored so that it may be quickly accessed when needed for use in the present. Numerous difficulties with IoT-based data storage in the cloud have been explored [9]. Utilising hash values to assure data storage spread optimisation in IoTs, cloud computing-based data storage has been optimised [10].

Fog computing is being used in a new green framework for IoT big data solutions in the healthcare industry. Low latency and delay allow for real-time access to the data [11].

Another innovative method for effective data management for IoT devices has been found. According to recover-ability and survivability, which offer resilience against network failure in the targeted region, the performance of the system has been assessed [12]. The data across fog nodes/ mini clouds inside the edge devices has been optimised using a distributed cloud-IoT approach. By properly aggregating and processing traffic, the suggested approach provides positive outcomes in terms of latency and energy consumption [13]. To process data locally by compressing it, the idea of edge computing integration with nodes that collect sensors has been introduced.

The integrated approach manages multiple monitoring, reconfiguration, and data adaptation operations to deliver effective outcomes with little or no communication overheads [14]. To handle the personal data of IoT devices, a secure retention and deletion strategy utilising key formation encryption and data analysis has been devised. The derivation key technique is used to encrypt the sensitive user data, guaranteeing data privacy while minimising page transmission overheads [15]. You can find further examples of modern authentication techniques produced by other scholars. [16] [17] [18]. With an emphasis on the effectiveness of registration, a mutual verification, agreement, and random node connect based smart card validation for WSNs was created [19]. Without the usage of a smart card, a different user-efficient authentication technique has been established, providing security versus insider threat, theft assault, and transaction recovery attack in any WSN [20].

A three-factor based authentication mechanism has also been implemented to enhance functionality, and it provides more privacy and identification in a specific WSN. The next notable project, called Automated Validation of the Security of Internet Protocols and Programmes (AVISPA), made use of formal vulnerability verification [21]. A different mutual authentication-based technique used biological data with hash and XOR algorithms to provide adequate password verification [22]. A multi-gateway WSN has recently been created to achieve increased security in the area of user-efficient authentication. The elements of the most well-liked methods, such as password authentication and biometric authenticators, are integrated in this novel way to provide the needed security. Additionally, this idea of bio-hashing has been further developed to eliminate the erroneous accept rates while effectively increasing the false rejection rate [23].

Numerous techniques were first presented in the case of WSN-based IoT systems authentication [24] [25] [26]. The next patch included two authentication systems, one of which uses a hash and the other of which uses an XOR computation to defend against various assaults [27]. The development of a safe data aggregation system for fog-assisted, WSN-enabled IoTs followed. Peer-to-peer (P2P) communication between sensing nodes is seen as sharing classified data with an aggregating node, which then broadcasts the information privately to a fog server [28]. To achieve identification, a simple multi-gateway WSN based IoT system has been designed. The authentication procedure in this approach has been completed in two steps: its "visit in" and the gateway's "out of scope" [29].

For WSN-based IoT, another authentication method uses user agreements to guarantee confidentiality for users. This approach eliminates a number of security issues and provides user anonymity without demanding complicated calculation. In addition, this scheme's user-friendly reciprocal authentication confirms the accuracy of the previous session key [30]. For current WSN-IoT contexts, a unique three-factor based authentication mechanism has been provided. This strategy avoids a number of security issues, including attacks involving stolen mobile devices, impersonation attacks, weak session key agreements, and improbability of the revocation process [31].

However, the decentralisation, indestructibility, transparency, and distributed decision features of block chain, an emerging technology, can enhance security performance [32] [33]. For safe and effective key management, a decentralised block chain-based keyless signature system has been created [34] [35]. For the privacy-preserving and consistency of automobiles in Vehicular Adhoc Networks (VANETs), another identification method based on the block chain has been suggested [36]. As a result, using the block chain in WSN to increase WSNIoT security through fog, cloud-based computing, or storage is a natural alternative.

e. As a first step in this direction, a block chain-based trust model has been created in WSNs for the identification of rogue sensor nodes. This concept uses a quadrilateral localization algorithm and a block chain with smart contracts to identify rogue nodes in a 3D environment. The outcomes of the consensus process are recorded on a distributed block chain [37]. Block chain technology is being used in WSNs to implement a novel trust-based safe localisation mechanism.

d is then the construction that is agreed upon [38] [39]. [40] [41] [42] [43] examines several further block chain applications for the Internet of Things. WSN is essential for the development of IoTs since they are made up of several sensing devices with a range of capabilities that may be used for numerous applications. WSNs are made up of several sensing devices with various functionalities that are placed in an area of interest. However, WSNs encountered a number of issues related to memory, power, safety, compute and communication costs, etc. The most important issue is how effectively to use memory, and protecting the confidential nature of stored data from unauthorised access is difficult.

As a result, BS uses registration and certification procedures to protect the confidentiality and authentication of sensor nodes. Additionally, the data is only gathered from verified sensor nodes and sent in the direction of clouds. Content stored in clouds is not shared with outside parties. According to the considerable literature, academics haven't looked as deeply into block chain-based solutions for authentication and privacy protection. Additionally, cloud-based data storage in WSNs is still in its infancy. As a result, the current method addresses the aforementioned problems.

The current research paper's major contribution is to provide a solution based on block chain with cloud storage for WSN-enabled IoTs. For authentication, the combined processes of certification and revocation are used, ensuring resilience against diverse assaults.

To overcome the aforementioned difficulties, a confidentiality based on a verification strategy for cloud computing is suggested.

After reviewing the prior study, it was possible to identify certain current issues, which were then addressed by the suggested plan, as indicated in Table I.

**EXISTING SYSTEM:**

However, before discussing the proposed network model and results obtained, recent literatures related to WSNs based IoT with blockchain technology are reviewed briefly for the data storage, authentication and security. The large amount data produced by IoT devices needs to be stored efficiently so that it can be easily retrieved on demand for real time usage. Various challenges during IoT-based data storage in cloud computing have been discussed. Cloud computing based data storage has optimized using hash values which ensure data storage distribution optimization in IoT. Another energy-efficient framework has introduced using fog computing for IoT big data solution in healthcare. The data can be accessible in real time with low latency and delay. Another novel approach has been identified for efficient data management for IoT devices. The performance of the scheme has evaluated in terms of recover-ability and survivability which provide robustness against failure of network within area of interest. Distributed cloud- IoT based solution has involved for optimizing the data among fog nodes/miniclouds within the edge devices. The proposed scheme offers promising results in terms of latency and energy consumption by proper traffic aggregation and processing. The concept of integration of edge computing with sensor nodes has adopted for processing of data locally by compressing the data quickly. The integrated scheme provides effective results which minimize communication overheads by

handling various monitoring, reconfiguration, and data adaption actions. A secure data management and deletion scheme has been introduced using key derivation encryption and data analysis to handle personal information of IoT devices. The sensitive user’s information is encrypted using derivation key algorithm which ensures the privacy of data with reducing the page transfer overheads optimally. Various authentication schemes have been recently developed by different researchers can be seen elsewhere. A mutual authentication, agreement and random node join based smart card authentication for WSNs was developed with particular emphasis on the efficiency of authentication. Another, user efficient authentication method has been introduced without using smart card which provided security against insider attack, theft attack and session recovery attack in any WSNs. Further, to improve the functionality,a three- factor based authentication method has been introduced and that accomplish more privacy and authentication in a particular WSNs. Automated Validation of Internet Security Protocols and Applications (AVISPA) was the next noticeable effort and that utilized formal security verification. Another variation of mutual authentication based scheme used biological information and utilized it with hash and XOR computations which offered sufficient password verification. In the category of user efficient authentication a multi-gateway WSN has been recently developed to accomplish enhanced security. In this exotic approach, the features of most popular schemes, like, password authentication and biometric authenticator are combined to achieve on the desired security. Also, this concept of bio-hashing has been further improved to eradicate the false accept rates without enhancing the false rejection rate efficiently.

Disadvantages: In the existing work, the system cannot resist number of attacks due to post methods used. This system is less performance in which an adversary may deny the contribution of transmitted and received messages or packets to produce confusion for trusted authority.

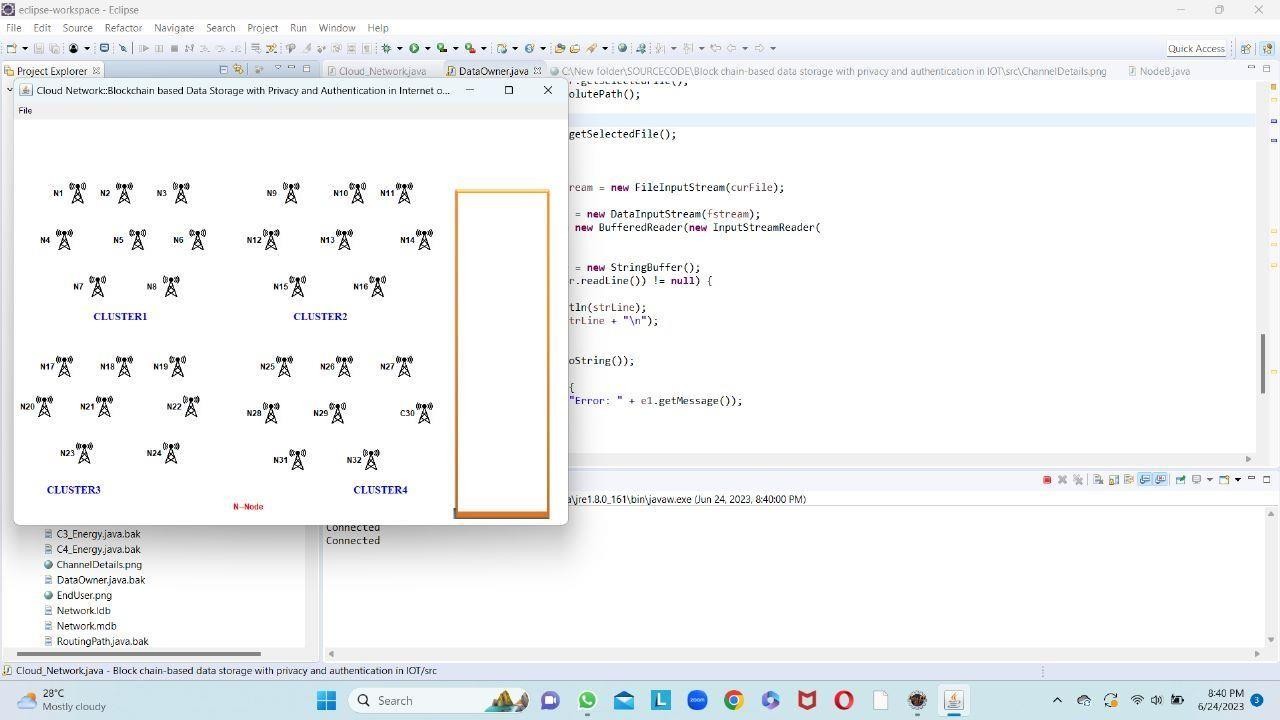
**PROPOSED SYSTEM:**

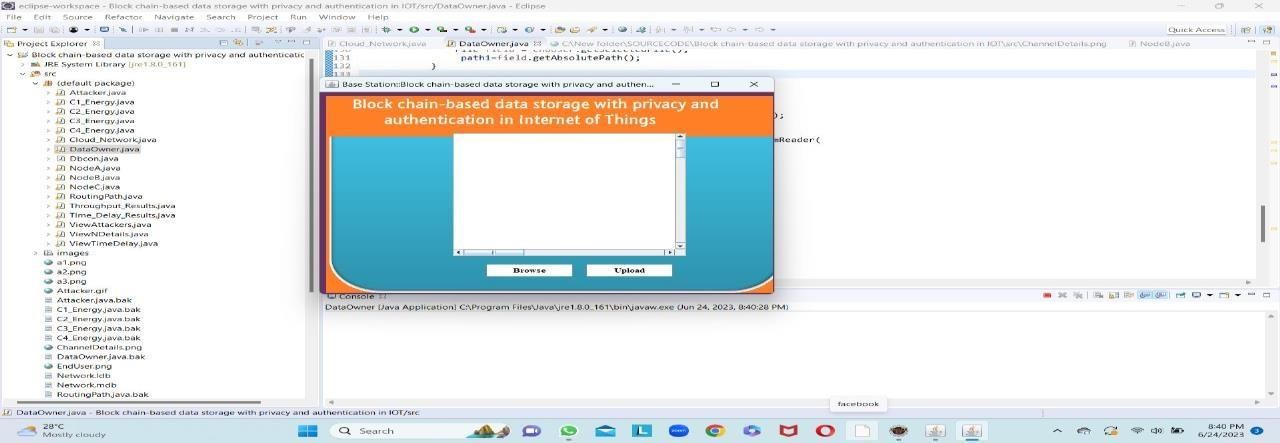
The proposed scheme is developed to address security concern using centralized database. Two types of sensor nodes are utilized in the proposed scheme such as regular sensor nodes RSN and cluster

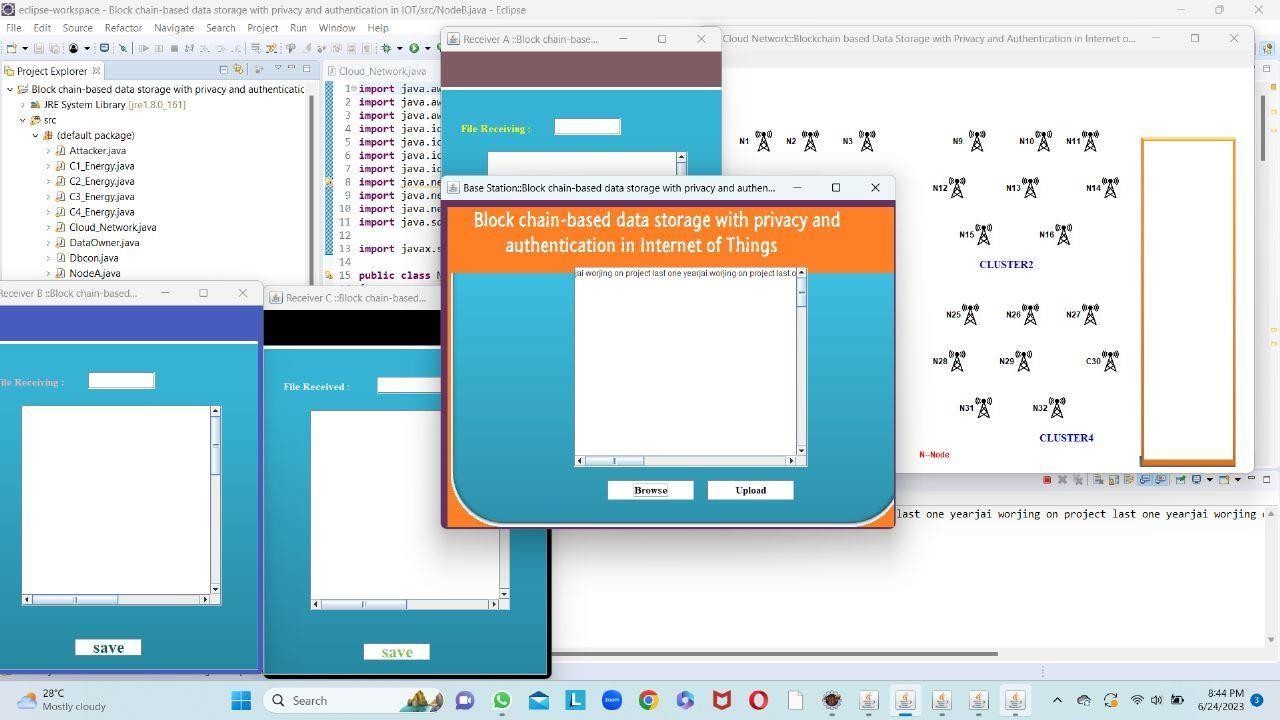
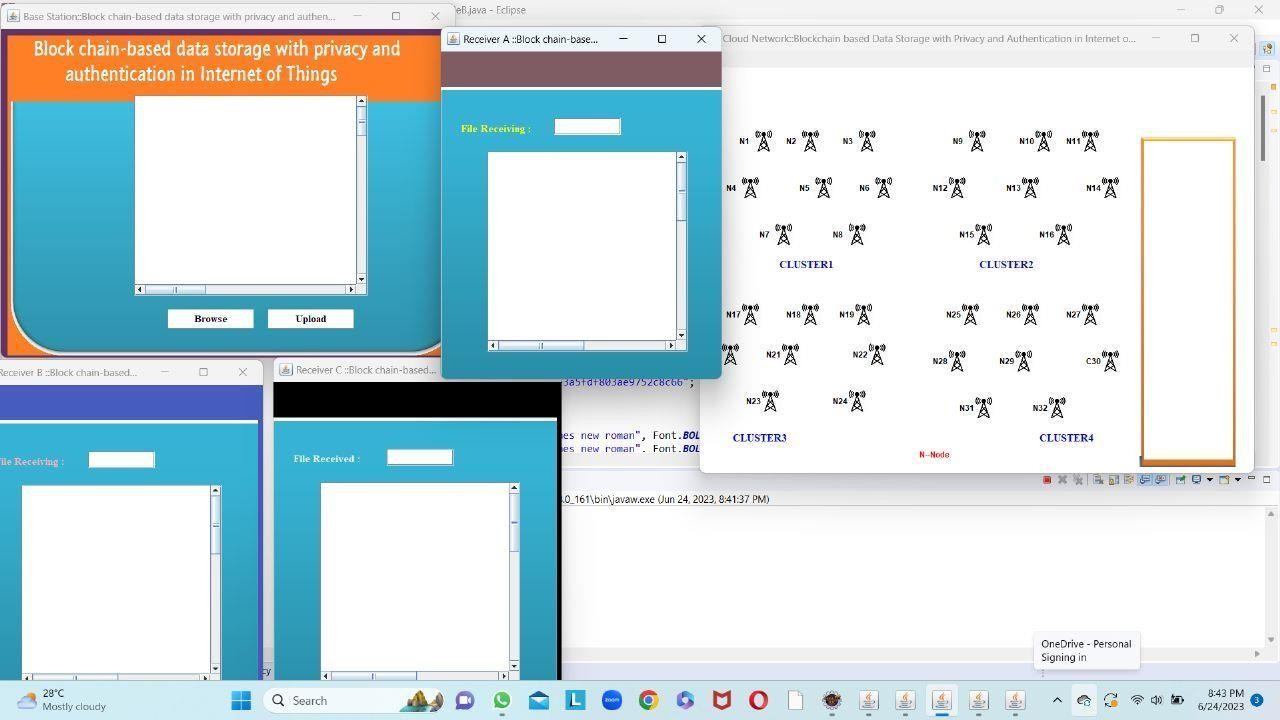
head sensor nodes CHSN. RSN are resource constrained in terms of energy, storage and processing capability. These sensor nodes sense phenomena happen surround and forward the gathered information to CHSN. CHSN is responsible for gathering information from RSN and forward information to Base station act as a Trusted Authority BTA. BTA is responsible for certification of all sensor nodes. Initially, the legitimacy of sensor nodes is granted by BTA before joining the network. Sensor nodes will get the authentication information and different parameters from BTA. Further, the sensor RSN forwards sensed information to CHSN. Further, the information is forwarded by CHSN towards BTA through wireless medium, therefore it is very easy for attackers to stole and forge the data such as location, speed, identity and sensed information during transmission. Hence, block chain based privacy-preserving scheme is proposed to mitigate such problems.  The proposed scheme is completed into various steps such as initialization phase, Registration phase, sensor node authentication phase, message signing and verification phase, key update phase and revocation phase and tracing phase. Initially, all the parameters required for all phases are computed by BTA. After that, all regular sensor nodes can initialize process by providing their information (like location, speed, identity, residual energy and sensed information) to CHSN. Further, CHSN broadcasts all information including its own information towards BTA. After collecting the information from CHSN, BTA utilizes that information to construct an untamperable Key Mechanism (UKM) and then allocates the UKM to all CHSN. Then, CHSN stored UKM and further keys are distributed among regular senor nodes.

Advantages: A block chain-based solution for privacy preserving and authentication with cloud storage, Base station provides certification to all sensor nodes, Certification key of all nodes are stored in an Untamperable Key Mechanism. Large amount of sensed information are stored in clouds.

**RESULT:**







**CONCLUSION:**

For the WSN-enabled IoTs, a block chain-based authentication mechanism with cloud data storage was successfully implemented. Initially, BS handled the registration and certification procedures for all sensor nodes. Following certification, all of the key parameters were kept in an Untameable Key Mechanism (UKM) that was under the control of the cluster heads. Additionally, the cluster heads broadcast the data that its members had collected to BS, where it was divided into two categories: essential parameters and sensed data. The vast quantity of data collected by these sensors was then uploaded to the cloud for more dependable and effective storage. To increase the immutability and transparency of the collected data, the critical parameters were later recorded using upcoming block chain technology.

Sensor nodes that weren't working properly were removed using the certification revocation process. In terms of detection accuracy, certification latency, and computing overheads, the suggested technique produced improved results. The simulation results and comparison analysis show that, in terms of average detection accuracy, the suggested method performs 19.33% better. The planned plan's dependability and efficacy were secured by the sharing of a significant volume of data into cloud storage. In the future, we'll aim to improve the framework's data management and resource usage for efficient outcomes.

**REFERENCES:**

[1] Y. A. Abdulrahman, M. Kamalrudin, S. Sidek, and M. A. Hassan, ”Internet of things: Issues and challenges,” Journal of Theoretical and Applied Information Technology, vol. 94, no. 1, pp. 52–60, 2016.

[2] SK Lo, Y Liu, SY Chia, X Xu, Q Lu, L Zhu, H Ning, Analysis of blockchain solutions for IoT: A systematic literature review, IEEE Access, vol. 7, 2019, pp. 58822-58835.

[3] R. V Kulkarni, S. Member, A. Forster, and G. K. Venayagamoorthy, ¨ ”Computational Intelligence in Wireless Sensor Networks: A Survey,” Communications Surveys & Tutorials, IEEE, vol. 13, no. 1, pp. 68–96, 2011.

[4] A. H. Bagdadee, M. Z. Hoque, and L. Zhang, ”IoT Based Wireless Sensor Network for Power Quality Control in Smart Grid,” Procedia Computer Science, vol. 167, pp. 1148–1160, 2020.

[5] J. Wang, Y. Cao, B. Li, H. jin Kim, and S. Lee, ”Particle swarm optimization based clustering algorithm with mobile sink for WSNs,” Future Generation Computer Systems, vol. 76, pp. 452–457, 2017.

[6] Z. Song-Juan and Y. Jian, ”Distributed data storage strategy in wireless sensor networks,” International Journal of Online Engineering, vol. 12, no. 11, pp. 52–57, 2016.

[7] L. Buttyan, D. Gessner, A. Hessler, and P. Langendoerfer, ”Application of wireless sensor networks in critical infrastructure protection: challenges and design options Security and Privacy in Emerging Wireless Networks,” IEEE Wireless Communications, vol. 17, no. 5, pp. 44–49, 2010

[8] R. Singh, D. K. Singh, and L. Kumar, ”A review on security issues in wireless sensor network,” vol. 2, no. 7, pp. 28–34, 2010.

[9] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, “IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges,” IEEE Internet of Things Journal, vol. 4, no. 1, pp. 75–87, 2017.

[10] M. Wang and Q. Zhang, “Optimized data storage algorithm of IoT based on cloud computing in distributed system,” Computer Communications, vol. 157, pp. 124–131, 2020.

[11] C. Feng, M. Adnan, A. Ahmad, A. Ullah, and H. U. Khan, “Towards Energy-Efficient Framework for IoT Big Data Healthcare Solutions,” Scientific Programming, vol. 2020, pp. 1–9, 2020.

[12] M. Asiri, T. Sheltami, L. Al-Awami, and A. Yasar, “A Novel Approach for Efficient Management of Data Lifespan of IoT Devices,” IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4566–4574, 2020.

[13] P. Maiti, J. Shukla, B. Sahoo, and A. K. Turuk, “Efficient Data Collection for IoT Services in Edge Computing Environment,” in Proceedings - 2017 International Conference on Information Technology, ICIT 2017, 2018, pp. 101–106.

[14] M. Adel Serhani, H. T. El-Kassabi, K. Shuaib, A. N. Navaz, B. Benatallah, and A. Beheshti, “Self-adapting cloud services orchestration for fulfilling intensive sensory data-driven IoT workflows,” Future Generation Computer Systems, vol. 108, pp. 583–597, 2020.

[15] J. Xiong et al., “A secure data deletion scheme for IoT devices through key derivation encryption and data analysis,” Future Generation Computer Systems, 2019.

[16] T. H. Chen and W. K. Shih, ”A robust mutual authentication protocol for wireless sensor networks,” ETRI Journal, vol. 32, no. 5, pp. 704–712, 2010.

[17] N. Bruce, Y. J. Kang, H. R. Kim, S. H. Park, and H. J. Lee, ”A security protocol based-on mutual authentication application toward wireless sensor network,” Lecture Notes in Electrical Engineering, vol. 339, pp. 27–34, 2015.

[18] K. Chatterjee, A. De, and D. Gupta, ”A Secure and Efficient Authentication Protocol in Wireless Sensor Network,” Wireless Personal Communications, vol. 81, no. 1, pp. 17–37, 2015.

[19] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, ”A dynamic password-based user authentication scheme for hierarchical wireless sensor networks,” Journal of Network and Computer Applications, vol. 35, no. 5, pp. 1646–1656, 2012.

[20] T. Maitra, R. Amin, D. Giri, and P. D. Srivastava, ”An effcient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card,” International Journal of Network Security, vol. 18, no. 3, pp. 553–564, 2016.

[21] A. K. Das, A. K. Sutrala, S. Kumari, V. Odelu, M. Wazid, and X. Li, ”An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks,” Security and Communication Networks, vol. 9, no. 13, pp. 2070–2092, 2016.

[22] H. Guo, Y. Gao, T. Xu, X. Zhang, and J. Ye, ”A secure and efficient three-factor multi-gateway authentication protocol for wireless sensor networks,” Ad Hoc Networks, vol. 95, 2019.

[23] J. Srinivas, S. Mukhopadhyay, and D. Mishra, ”Secure and efficient user authentication scheme for multi-gateway wireless sensor networks,” Ad Hoc Networks, vol. 54, pp. 147–169, 2017.

[24] F. Wu et al., ”An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment,” Journal of Network and Computer Applications, vol. 89, pp. 72–85, 2017.

[26] M. S. Farash, M. Turkanovic, S. Kumari, and M. H ´ olbl, ”An efficient ¨ user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment,” Ad Hoc Networks, vol. 36, pp. 152–176, 2016. [25] M. Turkanovic, B. Brumen, and M. H ´ olbl, ”A novel user authentication ¨ and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion,” Ad Hoc Networks, vol. 20, pp. 96–112, 2014.

[27] X. Zhang and F. Wen, ”An novel anonymous user WSN authentication for Internet of Things,” Soft Computing, vol. 23, no. 14, pp. 5683–5691, 2019.

[28] A. Ullah, G. Said, M. Sher, and H. Ning, ”Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN,” Peer-to-Peer Networking and Applications, vol. 13, no. 1, pp. 163–174, 2020.