Block Chain Based Data Storage With Privacy And Authentication In Internet Of Things

Mallu Mounika , Smt.K.R.Rajeswari, Sri.V.Bhaskara Murthy
MCA Student, Assistant Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

ABSTRACT

Internet of Things (IoTs) composed of large number of sensing devices with a variety of features applicable for various applications. In such scenarios, due to low data handling capabilities, limited storage and security aspects, it is quite challenging to protect networks against illegal information access and utilizes storage efficiently. Though researchers provide various solutions for security and data storage, but a few solutions are appropriate for WSNs enabled IoTs. Therefore, a blockchain-based decentralized framework integrated with authentication and privacy preserving schemes is developed for the secure communication in wireless sensor networks (WSNs) enabled IoTs. Registration, certification and revocation process are employed for the communication with sensor nodes and Base Station (BS) in a cloud computing environment. In this scheme cluster heads forward the collected information to the BS. Consequently, BS records all the key parameters on the distributed blockchain and large data is forwarded to clouds for the storage. The revoked certificates of all malicious nodes are eliminated from blockchain by BS. The performance of the proposed scheme is scrutinized in terms of detection accuracy, certification delay, computational, and communicational overheads. The simulated results, comparative analysis and security validation supports the superiority of the proposed solution over the existing approaches.

I. INTRODUCTION:

In current era, Internet of Things (IoTs) is one of the most popular, useful and dominant technologies in wireless communication and information processing [1]. IoTs is the formulation of 'things' that are distinguishable, understandable, manageable, and can be located with the help of the internet. In today's life, almost all things in IoT can be connected with internet owing to its communicational and computational capabilities, hence various more appropriate and suitable applications can also be realized [2]. Several sensor nodes are collectively deployed for monitoring, sensing and also for the automation purpose in IoT. The collection of these nodes are generally known as Wireless Sensor Networks (WSNs) and forms an inseparable part of IoT [3] as this technology can sense and monitor any physical things/activities within a particular environment.

The aforementioned sensor nodes, also known as 'motes', are cheap, tiny and are connected internally and distributed in specific areas [4]. These sensor nodes combine multi-features of sensing, computing and communication through wireless medium and hence in WSNs, physical phenomena are monitored and sensed in real time. Although, WSNs operation is applications specific in terms of the area of interest and way of deployment, but the final aim is monitoring, sensing, broadcasting and the processing of the collected information [5] [6]. However, the amount of information is huge with an extraordinary rate and that need to be addressed

in the current technological world. As known, WSNs are used in a variety of applications such as military, industry, smart home, healthcare, surveillance, habitat monitoring and agriculture to name a few. [7] [8]. Sensor nodes, the backbone of WSN, have limited resources such as energy, computational capability, storage, and communication bandwidth. So, when the demands of WSNs are gradually increases in IoT, more challenges are getting unearthed for the efficient use of it. Moreover, security is another most important concern in WSN enabled IoT. If an adversary attacks the network and deliberately compromised the nodes, the network security becomes a threat.

Therefore, it is required for WSNs to distinguish and eliminate malicious nodes from the network before becoming an active member in the IoT infrastructure. A. Summary of contribution Limited storage of sensor nodes, is an important research field and hence an effective and efficient storage of data is concern in WSNs when employed with IoT. Also, security is another most important concern in WSN enabled IoT. To address the above-mentioned issues of WSN in IoT, blockchain technology and cloud storage are incorporated for privacy preserving, authentication and storage. Blockchain-based solution integrates the authentication schemes with cloud storage for secure communication to WSNs, while the cloud storage itself disseminates the all storage limitation of sensor nodes. The main contributions of the proposed scheme are: 1) A block chain-based solution for privacy preserving and authentication with cloud storage, 2) Base station provides certification to all sensor nodes, 3) Certification key of all nodes are stored in Untamperable Key Mechanism 4) Large amount of sensed information are stored in clouds.

II. 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 [9]. Cloud computing based data storage has optimized using hash values which ensure data storage distribution optimization in IoTs [10]. 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 [11]. 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 [12]. 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 [13]. 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 [14]. 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 [15]. Various authentication schemes have been recently developed by different researchers can be seen elsewhere [16] [17] [18]. A mutual authentication, agreement and random node join based smart card authentication for WSNs was developed with particular emphasis on the efficiency of authentication [19]. 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 [20]. 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 [21]. Another variation of mutual authentication based scheme used biological information and utilized it with hash and XOR computations which offered sufficient password verification [22]. 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 [23].

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.

III. 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 gets 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

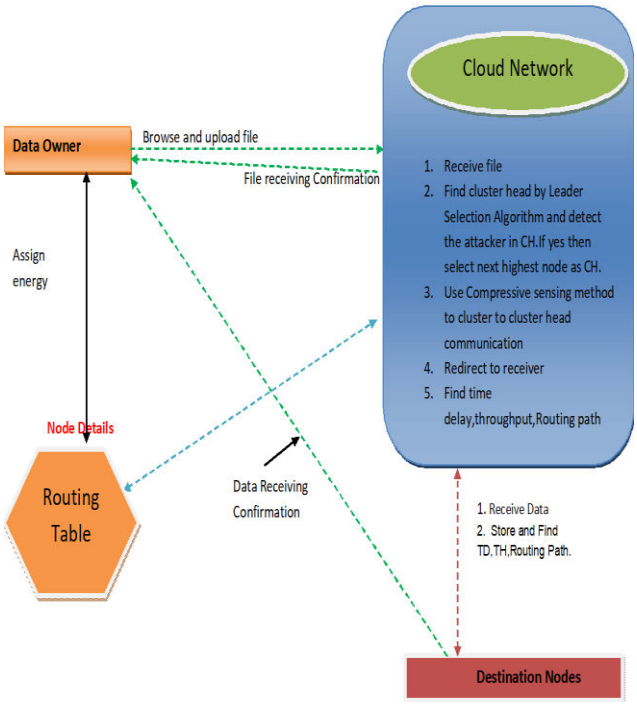
based privacy-preserving scheme is proposed to mitigate such problems.

- 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 a 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 Untamperable Key Mechanism
- Large amount of sensed information are stored in clouds.

IV. SYSTEM ARCHITECTURE:



V. MODULES:

- **Data Owner:**

  In this module, the Data Owner will browse the data file and then send to the particular Nodes. Data Owner will send their data file to router and router will connect to clusters, in a cluster highest energy sensor node will be activated and send to particular Nodes (A, B, C…). And if any attacker will change the energy of the particular sensor node, then Data Owner will reassign the energy for sensor node.

- **Cloud Network**

  The Cloud Network manages a multiple clusters (cluster1, cluster2, cluster3, and cluster4) to provide data storage service. In cluster n-number of nodes (n1, n2, n3, n4…) are present, and in a cluster the sensor node which have more energy considered as a cluster head and it will communicate first. In a router Data Owner can view the node details, view routing path, view time delay and view attackers. Router will accept the file from the Data Owner, the cluster head will select first and it size will reduced according to the file size, then next time when we send the file, the other node will be cluster head. Similarly, the cluster head will select different node based on highest energy. The time delay will be calculated based on the routing delay.

- **Cluster as Block Chain**
  In cluster n-number nodes are present and the clusters are communicates with every clusters (cluster1, cluster2, cluster3 and cluster4).In a cluster the sensor node which have more energy considered as a cluster head. The Data Owner will assign the energy for each & every node. The Data Owner will upload the data file to the router; in a router clusters are activated and the cluster-based networks, to select the highest energy sensor nodes, and send to particular Nodess.
- **Nodes (End User)**

  In this module, the Nodes can receive the data file from the Data Owner via router. The Nodes receive the file by without changing the File Contents. Users may receive particular data files within the network only.

- **Attacker**

  Attacker is one who is injecting the fake energy to the corresponding sensor nodes. The attacker decries the energy to the particular sensor node. After attacking the nodes, energy will be changed in a router.

VI. CONCLUSION:

A privacy-preserving authentication scheme based on block chain with cloud data storage was accomplished effectively for the WSN enabled IoTs. Initially, the process of registration and certification for all sensor nodes was performed by BS. After completing the certification process, all the key parameters were stored in Untamperable Key Mechanism (UKM) controlled by the cluster heads. Further, the cluster heads broadcast the collected information from its members to BS and the information is then separated into two parts, i) key parameters and ii) sensed information. The large amount these sensed data was then shared with cloud for more reliable and efficient storage. The key parameters were further recorded on emerging block chain technology to improve the immutability and transparency of the obtained data. The certification revocation process successfully eliminated malfunctioning sensor nodes. The proposed scheme accomplished better results in terms of detection accuracy, certification delay and computational overheads. The simulated results and comparative analysis demonstrate that the proposed algorithm achieves 19:33% better results in terms of average of detection accuracy. Sharing large amount of information into cloud storage ensured reliability and effectiveness of the proposed scheme. In future, we shall try to optimize the data management and resources of the framework for effective results.

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. F¨orster, 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. Turkanovi´c, 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. Turkanovi´c, 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.