# Study of Security Issues in Internet-of-Things using Blockchain Decentralized Authentication with Key Verification

Akash Kumar[1], Prof. Avinash Sharma[2]

[1]*PG Scholar,* [2]*Head and Associate Professor*

[1,2]*Dept. of CSE, MIT, Bhopal*

***Abstract;*** ***WSNs and IoT are having a self-organizing structure in which a large number of sensor nodes are randomly deployed in an area of interest to sense a particular physical activity. Two types of nodes take part in the localization process such as beacon nodes and unknown nodes or unaware nodes. The sensed information is broadcasted to the base station (BS) wirelessly from the beacon nodes, after receiving the information from the neighboring unknown sensor nodes. Different types of security threats for the proposed network model are: (i) broadcasting false location information, (ii) impersonation, (iii) tampering with the integrity of information, (iv) reports false energy information to misguide the trust evaluation process. 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 21.3% better results in terms of average of certification delay, 5.37% better results in terms of average of detection accuracy and 23.7% better results in terms of average of throughput. Sharing large amount of information into cloud storage ensured reliability and effectiveness of the proposed scheme.***

***Keywords: Nodes, Integrity, Computational, Tampering, Impersonation.***

## I. INTRODUCTION

The rapid evolution of the IoT market has caused an explosion in the number and variety of IoT solutions. Additionally, large amounts of funding are being deployed at IoT startups. Consequently, the focus of the industry has been on manufacturing and producing the right types of hardware to enable those solutions. In current model, most IoT solution providers have been building all components of the stack, from the hardware devices to the relevant cloud services or as they would like to name it as "IoT solutions", as a result, there is a lack of consistency and standards across the cloud services used by the different IoT solutions.

As the industry evolves, the need for a standard model to perform common IoT backend tasks, such as processing, storage, and firmware updates, is becoming more relevant. In that new model, we are likely to see different IoT solutions work with common backend services, which will guarantee levels of interoperability, portability and manageability that are almost impossible to achieve with the current generation of IoT solutions.

Creating that model will never be an easy task by any level of imagination, there are hurdles and challenges facing the standardization and implementation of IoT solutions and that model needs to overcome all of them.

## II. LITERATURE WORK

Rekha et. al, 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.[1]

Dr. S. Sobitha et. al, Property fraud is one big challenge in India and other developing countries. There have been

several instances of fraudulent acts corresponding to land such as forgery, credit frauds relating to bank loans. Hence we propose the usage of blockchain and smart contracts technology to counter these frauds. By using blockchain we can prevent forgery as it is immutable, the transfer of ownership can be done in a secure fashion by using smart contracts and finally we can solve the loan related issues pertaining to banks by assigning a dynamic credit score to the piece of land.[2]

Mohammed Amine Bouras et. al, Electronic healthcare (eHealth) identity management (IdM) is a pivotal feature in the eHealth system. Distributed ledger technology (DLT) is an emerging technology that can achieve agreements of transactional data states in a decentralized way. Building identity management systems using Blockchain can enable patients to fully control their own identity and provide increased confidence in data immutability and availability. This paper presents the state of the art of decentralized identity management using Blockchain and highlights the possible opportunities for adopting the decentralized identity management approaches for future health identity systems. First, we summarize eHealth identity management scenarios. Furthermore, we investigate the existing decentralized identity management solutions and present decentralized identity models. In addition, we discuss the current decentralized identity projects and identify new challenges based on the existing solutions and the limitations when applying it to healthcare as a particular use case.[3]

Hyung-Sin Kim et. al, Electronic healthcare (eHealth) identity management (IdM) is a pivotal feature in the eHealth system. Distributed ledger technology (DLT) is an emerging technology that can achieve agreements of transactional data states in a decentralized way. Building identity management systems using Blockchain can enable patients to fully control their own identity and provide increased confidence in data immutability and availability. This paper presents the state of the art of decentralized identity management using Blockchain and highlights the possible opportunities for adopting the decentralized identity management approaches for future health identity systems. First, we summarize eHealth identity management scenarios.[4]

Rekha Goyal et.al, A novel trust-based range-free secure algorithm using blockchain technology is considered in hostile WSNs for localization. The trust values of beacon nodes are evaluated against reputation value, mobility, residual energy and neighbor node list. The blockchain technology is implemented then to share the beacon nodes trust value with neighbor nodes. The highly trustworthy beacon nodes are subsequently elected as a miner for the mining process of blocks so that unknown nodes get information from highly honest beacon nodes to perform the localization process correctly. A set of simulations is conducted to validate the effectiveness of the proposed algorithm compared to the existing one. [5]

## III. PROBLEM IDENTIFICATION

The basic objections of my hypothesis work are according to the accompanying:

1. To reduce certificates delay during prevention then becomes message packets loss reduce respectively.

2. To improve detection accuracy then actual node detection becomes easier.

3. To improve throughput for efficient security issues in IoT.

## IV. OBJECTIVES

The basic objections of my hypothesis work are according to the accompanying:

1. To reduce certificates delay during prevention then becomes message packets loss reduce respectively.

2. To improve detection accuracy then actual node detection becomes easier.

3. To improve throughput for efficient security issues in IoT.

## V. PROPOSED METHODOLOGY

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 $CH_{SN}$. $R_{SN}$ are resource constrained in terms of energy, storage and processing capability. These sensor nodes sense phenomena happen surround and forward the gathered information to $CH_{SN}$. $CH_{SN}$ is responsible for gathering information from $R_{SN}$ and forward information to Base station act as a Trusted Authority $B_{TA}$. $B_{TA}$ is responsible for certification of all sensor nodes. Initially, the legitimacy of sensor nodes is granted by $B_{TA}$ before joining the network. Sensor nodes get the authentication information and different parameters from $B_{TA}$. Further, the sensor $R_{SN}$ forwards sensed information to $CH_{SN}$. Further, the information is forwarded by $CH_{SN}$ towards $B_{TA}$ 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, blockchain based privacy-preserving scheme is proposed to mitigate such problems.

***Algorithm: Blockchain Decentralized Authentication with Key Verification***

Phase I: Initialization Phase

Step 1: $B_{TA}$ generates ( $key_{pvt}^{TA}$ ) and ( $key_{pub}^{TA}$ )

Step 2: $B_{TA}$ computes ( $Enc_{pvt}^{TA}$ )

Step 3: Parameters computed {$K_G$, $TS(K_G)$ , $V_1$ and $V_2$}

Phase II: Registration Process

Step 1: $R_{SN}^{k} \rightarrow CH_{SN}^{j} : IN_i$ {location, speed, identity $(ID_{SN}^{K})$, residual energy and sensed information}

Step 2: $CH_{SN} \rightarrow B_{TA} : \left\{ ID_i, Password_{NM}^{i}, (Password_{NM}^{i} \oplus \varphi_i) \right\}$

Step 3: $B_{TA} \rightarrow CH_{SN} : \left\{ key_{pub}^{TA}, Enc_{pvt}^{TA}, SE_i, ID_i \; pID_i^{initial}, B_{TA}^{ID}, \varsigma 1_i, key_{secret}^{i}, iPad, oPad \right\}$

Step 4: $CH_{SN}^{j} \rightarrow UKM : \left\{ key_{pub}^{TA}, Enc_{pvt}^{TA}, SE_i, ID_i \; pID_i^{initial}, B_{TA}^{ID}, \varsigma 1_i, key_{secret}^{i}, iPad, oPad \right\}$

Phase III: Sensor Authentication Phase

Step 1: $UKM_j$ computes parameters

$\left\{ password^{k}, \varphi_k, password_{NM}^{k}, key_{secret}^{k}, \varsigma 1_k, \varsigma 2_k, Enc_{pvt}^{TA}, pID_k^{initial}, \varsigma 3_k \; and \; \varsigma 3_{kk} \right\}$

Step 2: $CH_{SN}^{j}$ check whether $\varsigma 3_k = \varsigma 3_{kk}$

Step 3: $CH_{SN}^{j}$ computes group key KG, $\gamma 1, \gamma 2$

Phase IV: Packet Signing

Step 1: Signing and verification of packets done by $CH_{SN}^{j}$

Step 2: $CH_{SN}^{j}$ generates a timestamp TSI and computes pseudo identity $\left\{ PID_{SN}^{K}, \sigma_i \right\}$

Step 3: $CH_{SN} \rightarrow B_{TA} : \{ I, PID_{SN}^{K}, \sigma_i, TS_I \}$

Phase V: Packet Verification Phase

Step 1: $B_{TA}$ verifies the freshness of packet by computing $\sigma_i^{*}$

Step 2: $B_{TA}$ check ( $\sigma_i = sigma_i^{*}$ )

Phase VI: Key Update

Step 1: $B_{TA}$ generate new $\{ K_G^{new}, TS_{(K_G)}^{new}, key_{(pvt_{new})}^{TA}, \gamma 1_{new}, \gamma 2_{new} \}$

Step 2: $B_{TA} \rightarrow stores < K_G^{new}, TS_{(K_G)}^{new}, \gamma 1_{new}, \gamma 2_{new} >$

Step 3: $B_{TA} \rightarrow CH_{SN} : \{ sign = sign_{(key_{pvt}^{TA})}(k) \}$

Step 4: $CH_{SN} \rightarrow UKM \{ Encryption_{(pvt_{old})}(k), key_{pub}^{TA} \; and \; TS_{(K_G)}^{new} \}$

Phase VII: Key Signing and Verification Process

Step 1: Generate new $CH_{SN} \rightarrow \text{Encryption}_{(\text{pvt}_{new})}(\text{key}_{pub}^{TA})$

Step 2: Check ( $\sigma_i = sigma_i^*$ )

Phase VIII: Revocation Process

Step 1: $B_{TA}$ blocks the ID of malfunctioning sensor nodes

Step 2: Legitimates sensor nodes computes $\{K_G^{new}, \text{key}_{(\text{pvt}_{new})}^{TA}\}$

## VI. RESULTS AND ANALYSIS

The performance of the proposed scheme is evaluated in terms of various metrics such as overheads, certification delay, detection accuracy, and throughput. These metrics play very important role during performance evaluation. The proposed scheme requires much less computation time and communication overheads as compared to existing schemes BDFAP[1]. The proposed scheme gives more effective results in terms of computation and communication overheads when compared with authentication and key agreement, public key based authentication and identity based authentication.

**Table 1: Impact of node density on certification delay (ms)**

| Number of Sensor Nodes | BDFAP[1] | BDAKV (Proposed) |
|---|---|---|
| 100 | 9 | 7 |
| 150 | 12 | 11 |
| 200 | 13 | 9 |
| 250 | 17 | 15 |
| 300 | 22 | 19 |
| 350 | 23 | 21 |
| 400 | 25 | 24 |

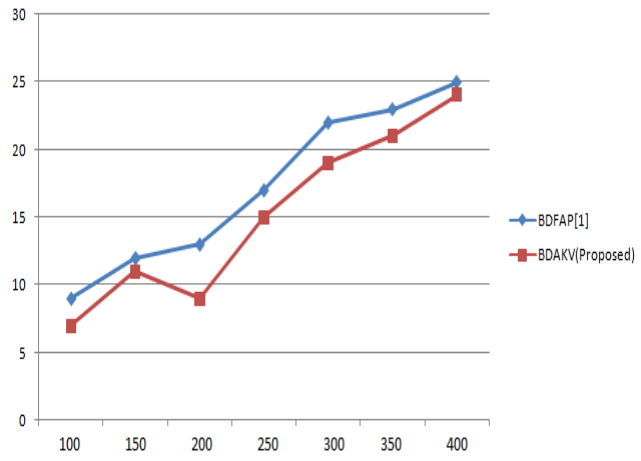


**Figure 1: Graphical analysis impact of node density on certification delay (ms)**

The proposed method BDAKV (Blockchain Distributed Authentication with Key Verification) performs outstanding result in case of certificate delay. When specify 100 sensor nodes then certificate delay of BDAKV is 7ms instead of 9ms. Similarly for 350 nodes, certificate delay of BDAKV is 21ms instead of 23ms.

**Table 2: Impact of simulation rounds on detection accuracy (%)**

| Simulation Time (Sec) | BDFAP[1] | BDAKV (Proposed) |
|---|---|---|
| 50 | 35.4 | 37.3 |
| 100 | 44.8 | 47.6 |
| 150 | 53.2 | 57.1 |
| 200 | 64.8 | 66.7 |
| 250 | 76.7 | 79.1 |
| 300 | 88.2 | 89.4 |
| 350 | 94.7 | 96.8 |
| 400 | 95.8 | 97.2 |

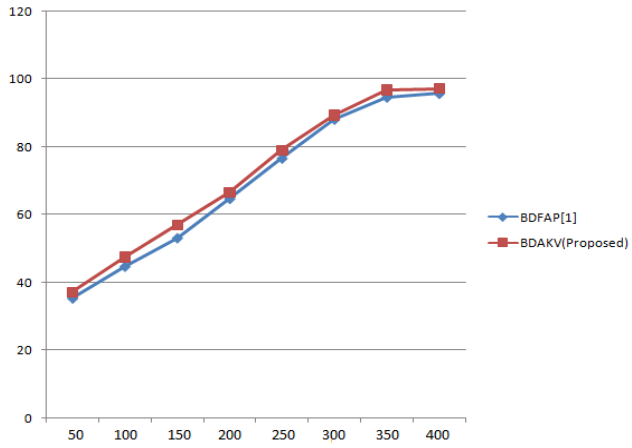


**Figure 2: Graphical analysis of impact of simulation rounds on detection accuracy (%)**

The proposed method BDAKV (Blockchain Distributed Authentication with Key Verification) performs outstanding result in case of detection accuracy. When

specify 100 Sec. simulation time then detection accuracy of BDAKV is 37.3% instead of 35.4%. Similarly for 350 Sec. simulation time, detection accuracy of BDAKV is 96.8% instead of 94.7%.

**Table 3: Impact of simulation time on throughput(%)**

| Simulation Time (Sec) | BDFAP[1] | BDAKV (Proposed) |
|---|---|---|
| 10 | 10.1 | 12.5 |
| 20 | 22.3 | 25.1 |
| 30 | 35.8 | 38.2 |
| 40 | 48.7 | 49.3 |
| 50 | 59.4 | 62.1 |
| 60 | 75.6 | 80.2 |
| 70 | 84.8 | 86.9 |
| 80 | 85.9 | 87.2 |
| 90 | 94.2 | 96.6 |
| 100 | 96.3 | 98.1 |

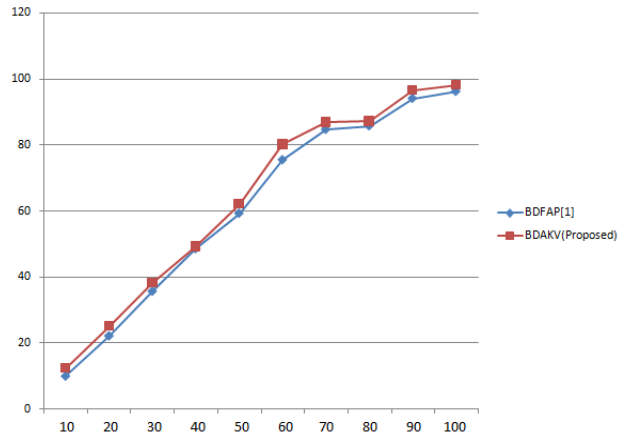


**Figure 3: Graphical analysis of impact of simulation time on throughput(%)**

The proposed method BDAKV (Blockchain Distributed Authentication with Key Verification) performs outstanding result in case of throughput. When specify 20 Sec. simulation time then throughput of BDAKV is 22.3% instead of 25.1%. Similarly for 100 Sec. simulation time, throughput of BDAKV is 98.1% instead of 96.3%.

## VII. CONCLUSION

A privacy-preserving authentication scheme based on blockchain 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 blockchain 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 21.3% better results in terms of average of certification delay, 5.37% better results in terms of average of detection accuracy and 23.7% better results in terms of average of throughput. Sharing large amount of information into cloud storage ensured reliability and effectiveness of the proposed scheme.

## VIII. FUTURE SCOPE

We shall try to optimize the data management and resources of the framework for effective results. The proposed algorithm efficiently further discriminates malicious beacon nodes and improves localization accuracy with resist network topology variety and localization ratio.

## REFERENCES

[1] Rekha Goyat, Gulshan Kumar, Rahul Saha, Mauro Conti, Mritunjay Kumar Rai, Reji Thomas, Mamoun Alazab, Tai Hoon-Kim, “Blockchain-based Data Storage with Privacy and Authenticationin Internet-of-Things”, IEEE Internet of Things Journal , 2020.

[2] Dr. S. Sobitha Ahila, Gajapathy. B, Deepanraj A. M, Jaishaanth. S, “Survey on Blockchain Based Document Digitization and Secured Storage ”, International Journal for Research in Applied Science & Engineering Technology, 2020.

[3] Mohammed Amine Bouras, Qinghua Lu, Fan Zhang, Yueliang Wan, Tao Zhang and Huansheng Ning, “Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective”, IEEE Journal of Sensors, 2020.

[4] Hyung-Sin Kim, “Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are”, MDPI Journal of Sensors, 2020.

[5] Rekha Goyat, Gulshan Kumar, Mritunjay Kumar Rai, Rahul Saha, Reji Thomas, Tai Hoon Kim, “Blockchain Powered Secure Range-Free Localization in Wireless Sensor Networks”, Arabian Journal for Science and Engineering, 2019.

[6] K. Salah, M. H. Rehman, N. Nizamuddin and A. Al-Fuqaha, “Blockchain for AI: Review and Open Research Challenges”, IEEE Access on Blockchain, 2019.

[7] Hongwei Zhang, Jinsong Wang, Yuemin Ding, "Blockchain-based decentralized and secure keyless signature scheme for smart grid", Springer Journal of Energy, 2019.

[8] Riaz Ullah Khan, Rajesh Kumar, Mamoun Alazab, Xiaosong Zhang, "A Hybrid Technique To Detect Botnets, Based on P2P Traffic Similarity", Cybersecurity and Cyberforensics Conference (CCC), 2019.

[9] Dong Zheng , Chunming Jing , Rui Guo , Shiyao Gao and Liang Wang , "A Traceable Blockchain-Based Access Authentication System with Privacy Preservation in VANETs", IEEE Access on Vanets, 2019.

[10] Wei She, Qi Liu, Zhao Tian, Jian-Sen Chen, Bo Wang and Wei Liu, "Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks", IEEE Access on Vanets, 2019.

[11] Tai-Hoon Kim, Rekha Goyat, Mritunjay Kumar Rai, Gulshan Kumar, William J. Buchanan, Rahul Saha and Reji Thomas, "A Novel Trust Evaluation Process for Secure Localization Using a Decentralized Blockchain in Wireless Sensor Networks", IEEE Access Journal of Cyber Security, 2019.

[12] Qinghua Lu, Xiwei Xu, Yue Liu, Ingo Weber, Liming Zhu, Weishan Zhang, "uBaaS: A unified blockchain as a service platform", Elsevier Journal of Future Generation Computer Systems., 2019.

[13] Claudio d, "Blockchain Support for Collaborative Business Processes", IEEE Spectrum on Blockchain, 2019.

[14] Amam Hossain Bagdadee, Md Zahirul Hoque, Li Zhang, "IoT Based Wireless Sensor Network for Power Quality Control in Smart Grid", International Conference on Computational Intelligence and Data Science, 2019.

[15] Sin Kuang Lo, Yue Liu, Su Yen Chia, Xiwei Xu, Qinghua Lu, Liming Zhu and Huansheng Ning, "Analysis of Blockchain Solutions for IoT: A Systematic Literature Review", IEEE Access Journal of Mobile Service Computing with Internet of Things, 2019.