Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1437–1446
DOI : 10.47974/JDMSC-1769

Blockchain enabled security mechanism for preventing data forgery in IoT-based smart homes

Arjun Singh [@]
Manipal University Jaipur
Jaipur
Rajasthan
India

Surbhi Chauhan [†]
Amity University
Noida
Uttar Pradesh
India

Shashi Kant Dargar
Department of Electronic Engineering
Kalasalingam Academy of Research and Education
Krishnankoil
Virudhunagar 626126
Tamil Nadu
India

Sumegh Tharewal [§]
Symbiosis Institute of Computer Studies and Research (SICSR)
Symbiosis International (Deemed) University
Pune
Maharashtra
India

[@] *E-mail:* `vitarjun@gmail.com`
[†] *E-mail:* `surbhichauhan2009@gmail.com`
[§] *E-mail:* `sumeghtharewal@gmail.com`

Vitthal Sadashiv Gutte [‡]
School of Computer Engineering and Technology
Dr. Vishwanath Karad MIT World Peace University
Pune
Maharashtra
India

Pradeep Kumar Tiwari [*]
Birla Global University
Gothapatna
Bhubaneswar 751029
Odisha
India

Sonam Gupta [#]
Ajay Kumar Garg Engineering Collage
Ghaziabad 201015
Uttar Pradesh
India

Abstract

Conventional homes have grown to be smart homes (SM) with the assistance of the Internet of Things (IoT). A unified gateway connects all Internet-enabled devices. Those gateways need to be secured by the usage of a sturdy safety method due to the fact safety is very vital. In order to conquer those problems, this observation shows employing Blockchain Technology (BC) for secured houses to make certain information private and safe. To cope with the safety problem with SH gateways, this paper proposes a solution. A reliable Q-learning algorithm with Blockchain assistance is proposed for the SH gateway to save data. three sections make up the protocol Q Learning Algorithm with Blockchain Support (QLABS). First, a Lattice cryptosystem based on Cipolla's extended Euclidean distance algorithm is used to record and store user data (CEED-LC). Second, while preserving data secrecy and integrity, the proposed cryptosystem offers a small Key Generation (KG) with excellent security. Third, with the assistance of QLABS protocol agreement, the blocks are created with a specific gateway enrolment-ID. The testing results demonstrate how highly safe the suggested framework is against the vulnerabilities by obtaining a higher throughput along with a higher Packet Delivery Ratio (PDR) value. The results show that the recommended approach tops other existing algorithms in terms of PDR and throughput.

Subject Classification: *68T42 Agent technology and Artificial intelligence.*

Keywords: *Gateway, Cipolla's extended euclidean distance based lattice cryptosystem, Smart homes, Data forgery, IoT, Block chain.*

[‡] *E-mail:* **drshashikant.dargar@ieee.org**
[*] *E-mail:* **pradeeptiwari.mca@gmail.com (Corresponding Author)**
[#] *E-mail:* **guptasonam6@gmail.com**

1. Introduction

Homeowner comfort, security, convenience, augmented quality of life, etc are offered by an SH which is an IoT integrated residence [1]. The basic platform of an SH network is deemed as IoT. It interconnects heterogeneous smart devices namely smartphones, and smart meters, along with wearable devices. The capability of facilitating and promoting people's lives and independent living is possessed by SH systems. Valuable technologies like activity monitoring and health assessment are offered by SH systems which have gained the focus of users along with device developers [2] [3]. The IoT and network environment of these SH are seen as critical elements. Embedded computers are primarily covered by the SH's network structure, which is linked to various IoT devices centered on the Internet. Communication is changing from wired to wireless [4] [5]. It is now feasible to manage other devices via gateways, both inside and outside the SH when contrasted to how users operated every device. But a gateway-oriented SH environment has been formed by this change [6] [7]. Huge benefits for homeowners and stakeholders are offered by Gateway-centered SH, and possible risks of malicious cyberattacks are posed which might endanger the user's security along with privacy [8] [9]. Highly centralized frameworks are the conventional solutions to these risks which are susceptible to different malicious attacks. Therefore, the required agility and scalability are lacking by those solutions for sufficiently applying them in the new field of decentralized SH applications and services [10][11][12].

For conquering the existing issues, a secure protocol called QLABS for the SH gateway is created to evade data forgery.

The proposed model was implemented using blockchain-based technology and investigated in terms of conventional security processes such as security reaction times and the correctness. The results of the analysis demonstrate that the designed security solutions outperform existing alternatives.

2. Proposed Secure Smart Home Gateway Using Pol Blockchain Protocol

The SH is formed collectively by numerous devices that are controlled along with monitored by communicating via the gateway. Privacy breaches are experienced by user data, device malfunctions are caused, and users are harmed in such a centralized network configuration. For addressing

this problem, a secure QLABS protocol is created by the work for the SH gateway to evade data forgery as exhibited in Figure 1.

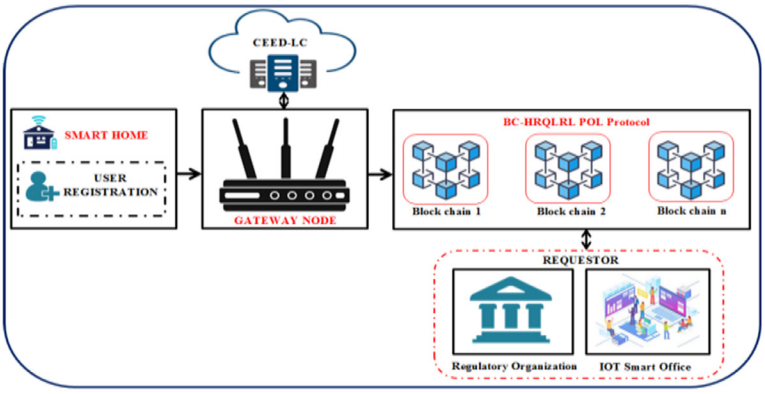


Figure 1

Proposed framework for secure smart home gateway

2.1 *User Registration*

In the registration phase, the user details are registered. User's name (Un_i^s), user's ID (Id_i^s), user contact number (Num_i^s), username (U_i^s), password generation (Pw_i^s), etc is the details that are registered into the SH gateway.

$$Reg(C_i^s) = \langle Un_i^s \,|\, Id_i^s \,|\, Num_i^s \,|\, U_i^s \,|\, Pw_i^s \,|\rangle \tag{1}$$

For the registered user, a username and password are generated by this registration phase to evade illegal access. Under gateway enrolment ID, the particular user details are saved in the server that is expressed as:

$$CS_i^S(GN_i^S) = Gen\langle UN_i^n \,|\, PW_i^n \,|\, GW_i^{ID}\rangle \tag{2}$$

The data are encrypted and centered on CEED-LC for securing the data as of attackers. The existing lattice cryptosystem utilizes the Extended-Euclidean-distance during the key-generation (KG) phase. Unfortunately, this approach leads to significant data expansion as the data is encoded on a bit-to-bit basis. To address this problem, a solution has been developed by combining Cipolla's algorithm with the Extended Euclidean distance algorithm. This merged algorithm effectively resolves the issue of data expansion by efficiently calculating the square roots of modular integers. Consequently, this enhancement improves key management performance

by reducing complexity while simultaneously ensuring higher security and availability for users.

(a) *Key Setup Phase*

A prime integer a such that $a \geq 2$ is initially chosen, co prime b is selected and c is indicated as the power of 2 that is selected such that $gcd(a,c) = 1$ and $gcd(b,c) = 1$ with $c > b$. Next, a polynomial set is considered $\{P(C), Q(C), R(C), S(C)\}$ with the degree $(a - 1)$, wherein, $P(C)$ indicates the secret key vector, $Q.(C)$ signifies the public key vector, $R(C)$ and $S(C)$ denotes polynomial-vectors.

A lattice $\Gamma(C)$ is formed by the consolidation of linearly independent vectors, which can be defined as follows:

$$\Gamma(C) = \sum_{i=0}^{P-1} (\Re_i C C^i \,||\, \Re_i \in Z_p) \tag{3}$$

$$\Im = \frac{Z[C]}{(C^P - 1)}, \Im_b = \frac{[[Z/Z_b][C]]}{(C^P - 1)^2}, \Im_c = \frac{[[Z/Z_c][C]]}{(C^P - 1)} \tag{4}$$

In this context, the notation:

$\{\Re_i\}$ indicates the set of integers, $\{C^i\}$ implies the set of vectors, and $\Im$ means convolution polynomial ring. $\Im$ is a matrix $p \times p$ that possesses the columns vectors. Vector coefficient are selected with the polynomial modulo r and modulo s in {-1,0,1} i.e. $\left(-\frac{ci}{2} \text{ to } \frac{ci}{2}\right)$ and $\left(-\frac{bi}{2} \text{ to } \frac{bi}{2}\right)$.

(b) *Key Generation Phase*

Cipolla's extended Euclidean algorithm is utilized to calculate both the secret key and the public key.

$$P(C)^2 P_b(C) = n.(\text{mod}\, b) \text{ which is } P(C)^2 = n.P_b(C)^{-1}(\text{mod}\, b) \tag{5}$$

$$P_b(C) = n.(P(C)^2)^{-1}(\text{mod}\, b) \tag{6}$$

$$P(C)^2 P_c(C) = n.(\text{mod}\, c) \text{ which is } P(C)^2 = n.P_c(C)^{-1}(\text{mod}\, c) \tag{7}$$

$$P_c(C) = n.(P(C)^2)^{-1}(\text{mod}\, c) \tag{8}$$

Where, P_b and P_c indicates the inverses of P.

Immediately the public-key and secret KG are assessed based on the Key Generation phase utilizing:

$$Pub_k(C) = [b.P_b(C)/(C)](\text{mod}\, c) \tag{9}$$

Where, $Pub_k(C)$ indicates a $p \times p$ matrix $\in Z_p$. Select a pair $(P(C)P_b(C))$,

$$Sk = \{P(C), P_b(C)\} \tag{10}$$

(c) *Data encryption*

Input parameters: $R(C)$ as well as $S(C)$ infers the polynomials vector with the maximum degree $(a-1)$, where $R(C)$, $S(C) \in Z_p$.

Compute ciphertext: $Cipher(C_i^s) = [R(C) + S(C)Pub_k(C)] \pmod{c}$ and save the encrypted $Cipher(U_i^s)$.

(d) *Data decryption*

Input parameters: $Cipher(U_i^s)$ and $P(C)$, public parameters, $Pub_k(C)$

Compute plaintext:

$$t(C) = P.(C)Cipher(C_i^s) \pmod{c} \tag{11}$$

$$t(C) = P.(C)[R.(C) + S.(C)Pub_k(C)] \pmod{c} \tag{12}$$

$$t(C) = P.(C)[R.(C) + S.(C)bP_b(C)/(C)] \pmod{c} \text{ as } [P.(C)P_b(C)] = 1 \pmod{c} \tag{13}$$

At last, the plain-text is estimated applying mod c as:

$$R(C) = [t(C)P_b(C) \bmod c]; \tag{14}$$

$R.(C) = [P.(C)R.(C)P_b(C)] \pmod{c.}$, and thus, it is identical to 0.

Similarly, $\gcd(P(C), P_b(C)) = 1 \pmod{c}$,

$$R(C) \pmod{c} = R(C) \tag{15}$$

At last, the plain text $R(C)$ is attained. In a gateway cloud server, the data received by the user are encrypted along with saved with a particular gateway enrolment ID (GW_i^{ID}).

3.2 *Gateway data management using blockchain*

The data transmission process's and records' integrity is guaranteed by a network composed of BC. Centred upon the essential information generated, the data created as of the end nodes taking part in the network are saved inside the BC utilizing the SHA-3 hash algorithm. On a BC

network node (N_D) within the cloud, these blocks are analogized in real-time. By identifying whether there exists a forged BC on the chain, they validate the data. Centred upon the individual gateway enrolment ID, the developed work primarily creates BC. Nowadays, employing QLABS, the network node or a smart agreement is verified. The networking resources together with the computing resources inside the computing servers are managed by the proof of learning-centred consensus and it improves the integrated resources utility. To compute the feedback that results in greater cost together with greater computation time, the conventional Q-Learning employs temporal difference for a long duration. Mean square error-based feedback evaluation is executed for resolving that issue. Centred on batch size, it validates the error, and the feedback is enumerated from every state and every action. All these are mathematically articulated as:

$$\Omega^{n+1}(\chi_t.(N_D), A_t.(N_D)) \leftarrow \Omega.(\chi_{t.}(N_D), A_t(N_D)) + \eta(R_t + \gamma \max_A \Omega(\chi_{t+1}(N_D), A) - \Omega(\chi_t.(N_D), A_t)) \quad (16)$$

Herein, η implies the learning efficacy; γ signifies the discount factor to balance immediate reward and long-term reward; $\Omega^{n+1}(\chi_t(N_D), A_t(N_D))$ symbolizes the novel value of the state $\chi_t(N_D)$ via an action $A_t(N_D)$; $\Omega(\chi_t(N_D), A_t(N_D))$ implies the old value; $\max_A \Omega(\chi_{t+1}(N_D), A)$ implies the optimum future value.

The proposed learning proof identifies the high-level $\Omega(\chi_t(N_D), A_t(N_D))$'s low-level characteristic via altering weights along with biases, (i.e.) $\Omega(\chi_t(N_D), A_t(N_D); w, B) \approx \Omega(\chi_t(N_D), A_t(N_D))$, wherein w and B signifies the sets of weights and biases within deep networks. For assessing the real value, the technique attempts to decrement the loss function during every training period. The loss function is equated as:

$$\forall(w, B) = \wp\left[R_t + \frac{\gamma}{n} \sum \max_{A'} \Omega(\chi'((N_D), A'(N_D); w', B') - \Omega(\chi_t(N_D), A_t(N_D); w, B))^2 \right] \quad (17)$$

Whilst there exists a slighter variance betwixt real $\Omega(\chi_t(N_D), A_t(N_D))$ and $\Omega(\chi'((N_D), A'(N_D)))$ predicted values, there exists a probability of efficient convergence and learning outcomes of deep networks. The learning outcomes are shared by every edge node once the networks are trained locally and arrive at an agreement with one another via the QLABS protocol. Herein, the summaries regarding the trained parameters within the deep neural network (DNN), together with the other needed records

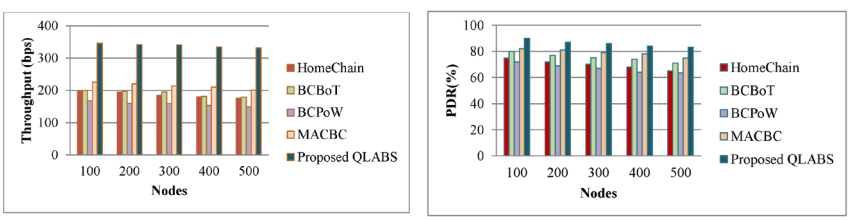
have been expressed as transactions, and via demanding distributed learning as of edge nodes, they enhance the whole learning performance.

Every node trains its network nodes locally within fixed time duration for keeping the learning outcomes database replications constant. Via the BC system, this fixed local training time has been set.

3. Results and Discussion

Centred upon diverse performance metrics, the proposed secure QLABS protocol's performance validation for a SH gateway for evading the data forgery is examined and analogized with the existent techniques for detecting the proposed methodology's efficacy. Centred upon the number of data nodes as of 100 to 500, the outcomes are assessed. In JAVA's functioning platform centred upon openly existent data comprising system configured Intel i5 processor, 3.20GHz CPU, along with 4GB RAM, the system is implied. Centred upon diverse performance metrics, namely throughput, Memory usage, PDR, together with execution time, the proposed QLABS protocol's valuation for the secured SH gateway is examined and analogized together with the Home Chain, BC-centred upon block-chain bubbles of trust (BCBoT), BC-based on proof-of-work (BCPoW), along with MAC centred BC (MACBC). Figure 2 graphically exhibits the throughputs and Packet delivery ratio's (PDR) evaluation.

The throughput metrics, which determine the transferred bits per second, is exhibited in Figure 2(a). It can be examined graphically that to exchange data for the incrementing sensor nodes (SNs), there exists discrimination in value. A greatly secured network constrains of the higher throughput value; whilst it is attacked by a few vulnerabilities, the value decrements. It is validated as of the graph that a throughput value ranging betwixt 346bps-332bps is attained by the proposed QLABS for the



(a) (b)

Figure 2

Graphical analysis of proposed QLABS based on (a) Throughput (b) PDR

SNs ranging betwixt 100-500, together with 341bps moderate throughput value for 300 SNs; this explicates that the proposed QLABS isn't that much vulnerable towards attacks. However, a throughput value ranging betwixt 149-226 bps is attained by the existent technique that signifies an insecure design.

Figure 2(b) showcases the PDR (Packet Delivery Ratio) validation, which calculates the ratio of the total number of packets successfully delivered from the source node to the destination node within the network, to the total number of packets sent. A higher PDR value signifies the maximal number of data packets, which have arrived at the destination. The network's performance increments as the PDR value increments. Thus, a PDR value ranging betwixt 83.20%-89.98% is attained by the QLABS, however, a total PDR value ranging betwixt 63.55%-79.99% is acquired by the existent technique that is comparatively lesser whilst analogized to the QLABS. Hence, the QLABS protocol stays to be secured against attacks; it sends the data onto the destination source with no data loss.

5. Conclusion

Specific challenges, like majority attacks, higher memory consumption, higher computation time, data loss, et cetera, are undergone by BC within IoT platforms. For the SH gateway to evade data forgery, the work has established a secured QLABS protocol. Substantial security against the vulnerabilities together with a secured centralized SH gateway under CEED-LC's and QLABS protocol's development is rendered by the developed work. Moreover, user's self-authentication is rendered by the work, and it also calculates within lesser usage along with lesser time. Experiential outcomes exhibit that a 332bps throughput and 83.20% PDR for 500 SN, the memory utilization of 2.88kb ROM, together with 9.86kb RAM is attained by the propounded QLABS, and whilst analogized to the existent work, it generally stays to be greatly secured and scalable.

References

[1] Minoli, Daniel. "Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach." Internet of Things 10, 100147 (2020).

[2] Dhoot, Anshita, Manisha Manjul, Sonam Kaul Devgan, A. N. Nazarov, and Pankaj. "Enhanced lightweight and secure session key establishment protocol for smart home inhabitants." *Journal of*

Discrete Mathematical Sciences and Cryptography 24, no. 5, 1327-1335 (2021).

[3] She, W. E. I., Zhi-Hao Gu, Xu-Kang Lyu, Q. I. Liu, Zhao Tian, and Wei Liu. "Homomorphic consortium blockchain for smart home system sensitive data privacy preserving." IEEE Access 7, 62058-62070 (2019).

[4] Malik, Vinita, and Sukhdip Singh. "Security risk management in IoT environment." *Journal of Discrete Mathematical Sciences and Cryptography* 22, no. 4, 697-709 (2019).

[5] Qashlan, Amjad, Priyadarsi Nanda, Xiangjian He, and Manoranjan Mohanty. "Privacy-preserving mechanism in smart home using blockchain." IEEE Access 9, 103651-103669 (2021).

[6] Saxena, Utkarsh, J. S. Sodhi, and Rajneesh Tanwar. "Augmenting smart home network security using blockchain technology." *International Journal of Electronic Security and Digital Forensics* 12, no. 1, 99-117 (2020).

[7] Fadhil, Saif Aamer. "Internet of Things security threats and key technologies." *Journal of Discrete Mathematical Sciences and Cryptography* 24, no. 7, 1951-1957 (2021).

[8] Yu, Zhihao, Liang Song, Linhua Jiang, and Omid Khold Sharafi. "Systematic literature review on the security challenges of blockchain in IoT-based smart cities." Kybernetes (2021).

[9] Ammi, Meryem, Shatha Alarabi, and Elhadj Benkhelifa. "Customized blockchain-based architecture for secure smart home for lightweight IoT." Information Processing & Management 58, no. 3, 102482 (2021).

[10] Hacid, Hakim, Wojciech Cellary, Hua Wang, Hye-Young Paik, and Rui Zhou, eds. Web Information Systems Engineering–WISE 2018. Cham: Springer (2018).

[11] Arif, Samrah, M. Arif Khan, Sabih Ur Rehman, Muhammad Ashad Kabir, and Muhammad Imran. "Investigating smart home security: Is blockchain the answer?." IEEE Access 8, 117802-117816 (2020).

[12] Singh, Pranav Kumar, Roshan Singh, Sunit Kumar Nandi, and Sukumar Nandi. "Managing smart home appliances with proof of authority and blockchain." In International conference on innovations for community services, pp. 221-232. Springer, Cham (2019).

[13] Sharma, Gajanand, Naveen Hemrajani, Satyajeet Sharma, Aditya Upadhyay, Yogesh Bhardwaj, and Ashutosh Kumar. "Data management framework for IoT edge-cloud architecture for resource-constrained IoT application." *Journal of Discrete Mathematical Sciences and Cryptography* 25, no. 4: 1093-1103 (2022).