EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Blockchain-Assisted Authentication and Energy-Efficient Clustering Framework for Secure IoT Communication

Madhu G.C.[1,*], Vijayakumar Peroumal[2*]

[1]Research Scholar, School of Electronics, Vellore Institute of Technology, Chennai, India.
[2]Professor, School of Electronics, Vellore Institute of Technology, Chennai, India.

Abstract

Securing sensitive information is a challenging task in an IoT environment due to the resource constraints of edge devices. Simultaneously, ensuring energy-efficient communication is equally important in clustered IoT networks. Resource depletion impacts the overall network lifetime. Existing methodologies treat authentication and routing as separate tasks, which leads to security vulnerabilities. Many existing authentication techniques use centralized control and static key management and are therefore vulnerable to various kinds of attacks including impersonation and brute force attacks. To address these issues, a blockchain based decentralized authentication and privacy-preserving framework for clustered IoT networks is proposed in this paper. A Trusted Domain Authority (TDA) enforces authentication among IoT devices, users, and gateways. It securely stores the authentication credentials of these entities in the blockchain and creates dynamic session keys for the Cluster Heads(CHs). The clusters are formed using a ranking-based K-Nearest Neighbour (KNN) algorithm. Reward-based Deep Q-Learning (OR-DQL) selects optimal CHs by using energy, vicinity, and trust as parameters. Additionally, the proposed framework safeguards packet headers from traffic analysis using a bounded Laplace differential privacy mechanism. The TDA generates dynamic session keys using Chinese Remainder Theorem (CRT) and securely distributes them to the CHs using the lightweight PRESENT cipher. The proposed system is implemented on the NS-3 network simulator. The simulation results demonstrate an improvement in throughput by 30.7%, a reduction in energy consumption by 24%, and a reduction in end-to-end delay by 27.7% compared to protocols such as ESMR and PBA. These results confirm that the suggested system can provide energy efficient secure communication in IoT networks.

Keywords: Authentication, Blockchain, Cluster Head, Differential Privacy, Internet of Things, Lightweight encryption.

Received on 10 June 2025, accepted on 16 August 2025, published on 8 December 2025

doi: 10.4108/eetiot.9520

1. Introduction

Critical IoT applications such as healthcare and smart cities exchange large volumes of sensitive data. It is essential to provide strong security measures to protect this data. Attackers often try to intercept the data transmitted over unsecured wireless links [1]. The most common types of attacks include impersonation, eavesdropping, data tampering, and man-in-the-middle attacks. However, most IoT devices have less computational power, battery, and memory [23]. Therefore, it is not feasible to implement advanced cryptographic techniques on these devices. Authentication prevents the illegal participation of entities in communication [2]. A secure authentication layer enables sensor nodes to transmit their data to gateways or cloud servers without being exposed to malicious attacks [3].

*Corresponding author. Email: vijayrgcet@gmail.com

Authentication schemes can range from simple credential-based identifiers such as passwords, biometric data, and other physiological features to advanced device specific hardware identifiers. Even though biometric authentication offers superior security, it is a difficult task to collect biometric information. Also, it can impose privacy issues. Recent techniques verify the identity of devices using their distinct unclonable hardware-based identifiers, called physical unclonable functions (PUFs) [4]. The PUFs exploit inherent manufacturing variations to create a unique identifier that serves as an unclonable fingerprint. The centralised authentication schemes are often prone to security vulnerabilities. If an attacker is successful in compromising the central authority, then the entire system will be compromised and disrupted. Static key management is another notable limitation that makes the system more vulnerable to attacks. To address this limitation, techniques for using time-bound dynamic keys have come into existence. However, these techniques introduce synchronization problems. Along with secure authentication, communication efficiency in IoT networks must also be considered. WSNs form the fundamental communication backbone for IoT networks. Ensuring energy-efficient communication is one of the important issues in IoT-based WSNs. Clustering improves energy efficiency as well as the network lifetime [5][25]. Some clustering schemes adopt simple CH selection criteria such as fixed rotation and proximity to the centroid. These approaches do not result in optimal CHs. Parameters such as energy, trust, distance, and delay should be considered when selecting stable CHs. The most common practice followed during data transmission is to encrypt the data payload while the header remains unencrypted. If the header is encrypted, intermediate network devices cannot identify the critical routing information such as source and destination addresses, number of hops, and other forwarding details. Due to this vulnerability, an attacker can perform traffic analysis to infer sensitive details such as the frequency of communication, locations of the communicating entities, and their communication patterns [6]. To address the above-mentioned limitations, we propose a Secure Blockchain-assisted Authentication and Clustering framework (BACS).

1.1. Contributions

The major contributions of this paper are as follows:

- We propose a Secure Blockchain-assisted Authentication and Clustering framework (BACS), which integrates blockchain for decentralization, multilayer authentication for security, Differential privacy-assisted header protection to prevent traffic analysis, and machine learning-based clustering and CH selection to improve energy efficiency.
- IoT users, devices, and gateways are verified using their device specific identifiers. These credentials are saved on a private blockchain maintained by Trusted Domain Authority (TDA). After successful verification of all the entities, a session key is supplied for the CH for secure communication.
- The TDA generates session keys using the Chinese Remainder Theorem (CRT) and Logistic chaotic map. The session keys are encrypted using the PRESENT cipher, and the symmetric keys used for encryption are derived from device-specific PUFs.
- To mitigate traffic analysis, we implemented Differential privacy (DP) for packet headers. A BBN is implemented to assess the sensitivity of the packet header, based on which the appropriate amount of noise to be injected is decided adaptively.
- An Optimal Reward-based Deep Q-Learning (OR-DQL) is used to create an energy and trust aware clustering. Mechanism. CHs are chosen dynamically by evaluating factors such as node's trust level, remaining energy, and mobility.

BACS is compared against ESMR and PBA with respect to energy consumption, throughput, and end-to-end delay. The remainder portion of this manuscript is arranged as follows: Section 2 highlights the pros and cons of the related literature. Section 3 discusses the architecture of the BACS. The results and comparative study are explained in Section 4. Section 5 concludes this study along with future research directions.

2. Related work

Many studies have investigated secure communication techniques for IoT settings. Mandal et al. (2020) introduced a three-factor authentication that verifies the communicating entities. A trusted gateway is used to coordinate device authentication Signcryption is the technique adopted to eliminate the dependency on certificates [7]. Though this method is effective, it follows a centralized approach, which limits its suitability for highly scalable applications and results in single point failures. Sathyadevan et al. (2019) developed the Protean based Authentication (PBA) for the edge nodes connected in IoT LAN. To prevent the cloneable attacks and device tampering their method relies on time bound dynamic keys for authentication. Since no static keys are involved, their method resists replay attacks [8]. Even though this method is effective in preventing cloning and replay attacks, it requires synchronization to track and use the dynamic keys. This method fails to detect anomalies in network. Haseeb et al. (2019) proposed an energy-efficient multi-hop routing technique for IoT-based WSNs that relies on a secret sharing (ESMR) scheme [9]. The Base Station (BS) is placed in a central position, and the network is organized in the form of circular zones. k-Nearest Neighbours algorithm is used to form clusters, and the CH selection is based on its proximity to the centroid of the cluster. The BS generates session keys for each zone's CH. The session keys are transmitted as plaintext, which creates an opportunity for attackers to intercept them and gain access to the session data. An additional disadvantage is the CH selection technique. The CHs are selected near the cluster centroid, which results in faster energy depletion of those nodes and consequently reduces the network's operational lifetime. To extend network lifetime, CHs need to be selected carefully by considering factors such as residual energy, mobility, delay,

distance, and trust [26]. The protocol does not have built-in session-key generation method or node-level authentication, which exposes the network to several attacks.

To safeguard data on Industrial IoT (IIoT) environments Fang et al. (2020) proposed an approach that uses a conditional proxy re-encryption technique. The system is resistant to several well-known security attacks in IIoT settings when re-encryption and controlled access are implemented [10]. With a centralized control model, it is difficult to manage IIoT infrastructure that spans multiple domains. In such cases, domain-specific administration and security may need to be managed by separate authorities.

For secure communication in heterogeneous IoT environments, Luo et al. (2020) proposed a privacy-preserving protocol. It demonstrates resistance to device-capture attacks. They employ a logistic map to generate session keys and rely on symmetric encryption [11]. A central server handles session management and device authentication. Even though the system shows decent performance in small-scale deployments, as the number of devices increases, its performance deteriorates. Also, depending on a single centralized server for authentication introduces a single point of failure.

A hybrid blockchain model was presented by Cui et al. (2020) to handle authentication in clustered IoT networks by combining public and private blockchains. A base station handles inter-cluster authentication, while CHs manage intra-cluster communication [12]. Although the system enhances decentralization and scalability, miner-based validation and dual-layer verification raise processing overhead and latency, making it inappropriate for IoT devices with limited resources. Existing methodologies, however, mostly address authentication or clustering in isolation, offer no adaptive protection for packet headers, and demonstrate limited scalability across multiple domains. To bridge this gap, we suggest a Secure Blockchain-Assisted Authentication and Clustering (BACS) framework which integrates multi-entity authentication, energy and trust aware cluster formation, and differential privacy-based header protection, and resource-efficient communication in IoT environments.

3. Proposed Model

The proposed system comprises IoT devices, users, gateways, and cross-domain TDAs. The BACS framework is depicted in Figure 1. Each domain maintains its own TDA to verify the identities of the IoT device, user, and gateway. As shown in Figure 2, the IoT devices are authenticated using the combination of device specific PUF and MAC addresses. The users are verified using their passwords and biometric features. Gateways are authenticated using a challenge response protocol and nonces. All the credentials are securely stored in a blockchain. When an entity initiates a login, the TDA validates its identity by retrieving the corresponding stored credentials from the blockchain. Every key distribution and login activity is hashed and added to the blockchain ledger. To prevent unnecessary overheads only the essential authentication information is maintained on-chain. After authentication, communication happens through encrypted links. Compared to the public blockchains, the permissioned blockchains offers scalability, less overhead and latency. Hence these blockchains are suitable for resource constrained IoT environments [13]. In this work, the TDAs utilize a permissioned blockchain for authentication. The framework supports inter-domain communication through verified gateway connections. The Storage Server functions as a centralized data repository for domain information.

3.1. Optimum Cluster Head Selection

The proposed system adopts a cluster-based environment to minimize complexity, reduce energy consumption and overhead associated with packet transmission and control message forwarding. Figure 3 illustrates the proposed Energy and Vicinity-aware Clustering (EV-C) mechanism. Clusters are formed using a ranking-based K-Nearest Neighbour (K-NN) classification algorithm [14]. Once the clusters are formed, the TDA generates a session key for the CH, which is elected using the Optimal Reward-based Deep Q-Learning (OR-DQL). Ranking based K-nearest neighbour algorithm is used to form the clusters, which elects the clusters based on the Lorentzian distance metric. The calculation of Lorentzian metric is defined as follows,

$$P = [P1, P2, \ldots . Pl]$$
$$Q = [Q1, Q2, \ldots . Ql]$$
$$Dis(P, Q) = \sum_{i=1}^{l} |P_i - Q_i| \quad (1)$$

Where, $Dis(P, Q)$ represents Lorentzian distance between

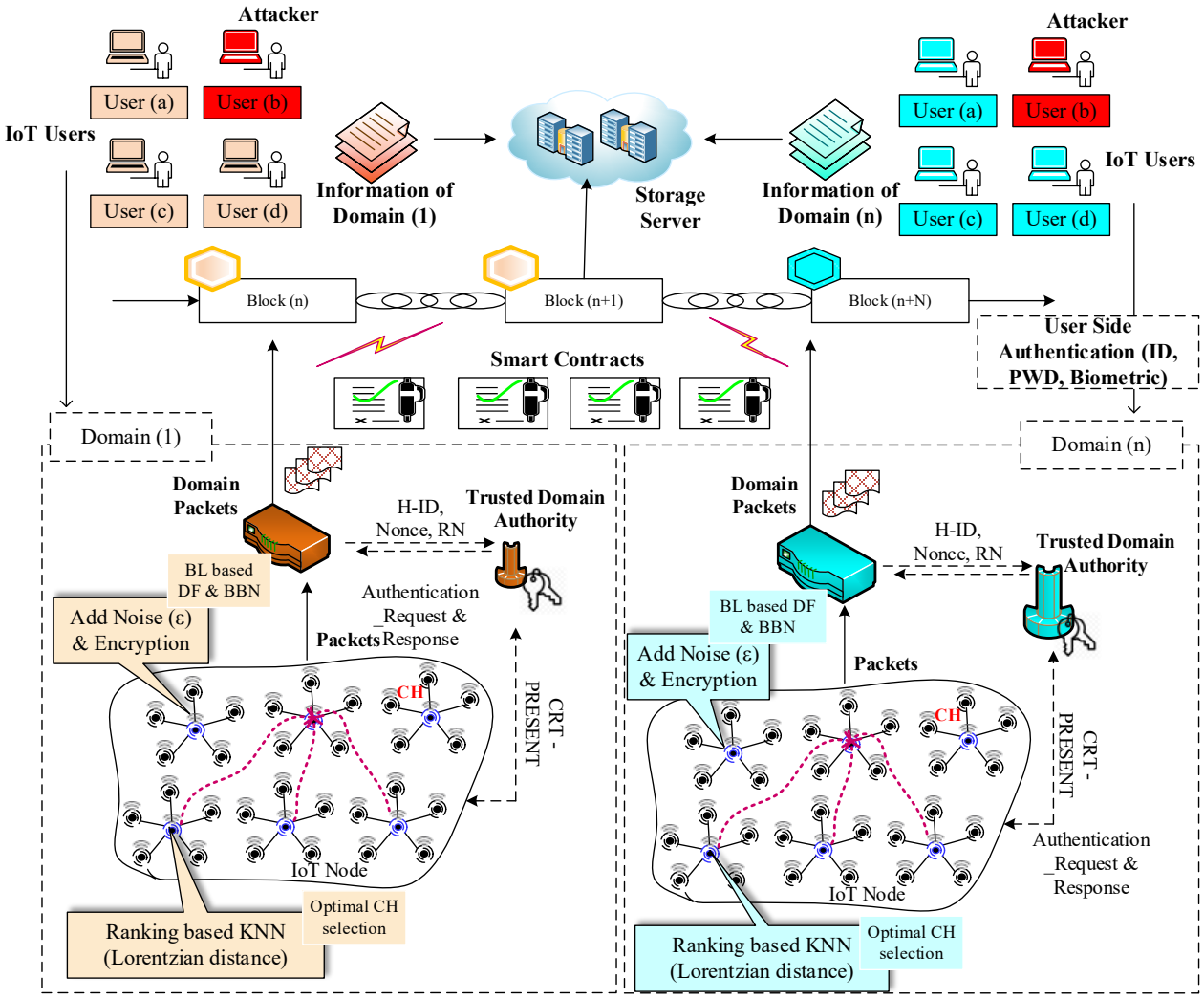

Figure 1. System Model of the BACS Framework for Secure Cross-Domain IoT Communication.

neighbor nodes. The K-Nearest Neighbor algorithm is used to identify the k nearest neighboring nodes of a given node by considering energy status, number of neighbors, trust, vicinity, mobility, and distance. After forming the cluster, the CH is elected using the OR-based DQL algorithm, which is managed by the gateway.

Algorithm 1. K- Nearest Neighbour

Step 1: Initialize flag ← 0, COUNT ← 0, H ← empty list of size k+1
Step 2: For each candidate point c_i:
Compute lower bound distance a[i] using hyperplane projection
Step 3: Sort a [ ] in ascending order → (a_sort[], index_sort [])
Step 4: While flag = 0 do
Step 5: i ← index_sort [count]
h ← calculate_kNN (a, H, i)
Step 6: Update H with h if closer neighbors found
Step 7: aknn ← maximum distance in current H.
Step 8: count ←count + 1
Step 9: If count ≥ k and aknn < a_sort[count] then
flag ← 1 // Search can be stopped early
End While

Mobility

Mobility represents the movement of IoT nodes and is a critical factor in dynamic network topologies. High mobility can cause issues such as route failures and miscommunication, due to frequent changes in network structure. The mobility of a node is calculated as follows:

$$M_{n_i} = \frac{1}{X}\sum_{x=1}^{X}\sqrt{(p(x)-p(x-1))^2+(q(x)-q(x-1))^2} \quad (2)$$

Where M_{n_i} represents nearest node mobility, $p(x)$ and $q(x)$

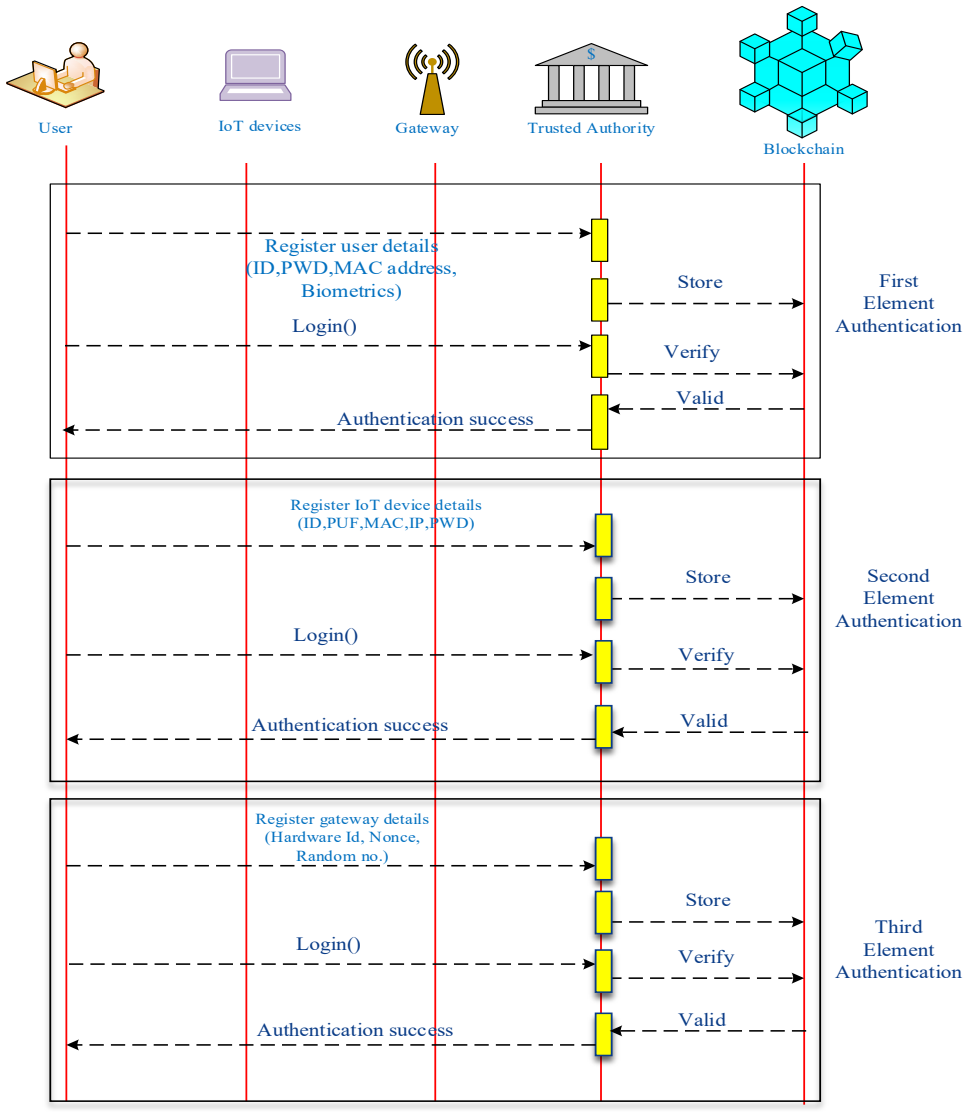

Figure 2. Three-Element Authentication Process in BACS framework.

represent the x and y coordinates of the node at time x. $p(x-1)$ and $q(x-1)$ are the coordinates at the previous time step $x-1$. X is the total number of time intervals.

Energy

It defines the remaining energy level of an IoT device. It is calculated by subtracting the energy consumed from the node's initial energy.

$$E = 1 - E_C \tag{3}$$

The energy consumed by node n, denoted as $EC(n)$, is defined as

$$EC(n) = \left[Tp \times \frac{Ds}{Dr} + Rp \times \frac{Ds}{Dr}\right] + N \times Loss \tag{4}$$

Where $EC(n)$ represents energy consumption of the node n, Tp represents transmission power, Ds is the size of the data and Dr is the data rate, Rp represents the receiver power.

Node Density

Node density is an important factor for determining a node's suitability in the clustering process. However, just counting neighbours is not correct, a node might have too few or too many, which can affect performance. To normalize this, the Relative degree R_d is calculated which measures the deviation of a node's density from the expected ideal density

$$R_d = |n_d - \sqrt{N}| \tag{5}$$

Where n_d is the actual number of neighbours for a node, N is the total number of nodes in a network.

$$N_F = \begin{cases} 1, & if\ R_d < \delta \\ x, & otherwise \end{cases} \tag{6}$$

If $N_F = 1$, the node is eligible for clustering.
The OR-DQL module considers four key parameters, residual energy, mobility, trust score, and relative node density to define the state space. A reward function is dynamically computed for each node. Using an ε-greedy policy, the agent selects actions to build the optimal CH set. The Q-values are updated using the Bellman equation, ensuring that CHs with strong reliability and energy efficiency are progressively reinforced [15]. The learning process halts when convergence in Q-values or cluster head selections is achieved.

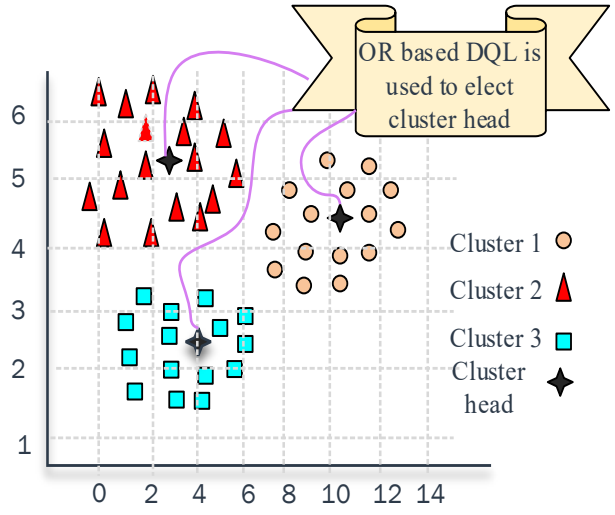

Figure 3. Energy and Vicinity aware clustering

Algorithm 2. OR-DQL-Based CH Selection in BACS

Step 1: Initialize Q-table Q(s,a), learning rate α, discount factor, and exploration rate ϵ
Step 2: For each training round do
2.1 Form clusters using K-NN
2.2 For each cluster do
a) Generate list of eligible CH candidates
b) For each candidate node i do
i. Construct current state S_i using: Residual energy, Trust score, Mobility score and Relative density.
ii. Choose action a_i using ε-greedy policy
iii. Simulate the action and compute reward $\boldsymbol{r_i}$
iv. Observe new state s′.
v. Update Q-value using:
$Q(S_i, a_i) \leftarrow Q(S_i, a_i) + \alpha[r_i + \gamma . \max_{a'} Q(S', a') - Q(S_i, a_i)]$
Step 3. Repeat until Q-values converge or maximum rounds reached.
Step 4. Select top nodes with highest Q-values as final CHs

3.2. Differential Privacy

In this research, we adapted Differential Privacy (DP) which is used to ensure privacy by adding noise to sensitive data. [16][17]. Bounded Laplace mechanism is used to dynamically select privacy budget parameter ε. To improve privacy, the suggested method uses a Bayesian Belief Network (BBN) to estimate data sensitivity based on probabilistic relationships and network context before noise is injected. A BBN is a probabilistic graphical model that represents the conditional dependencies among random variables using a Directed Acyclic Graph (DAG). The conditional probability of two random variables is defined as follows,

$$Prob(P|Q) = \frac{Prob(P,Q)}{P(Q)} \tag{7}$$

If P and Q are independent, then

$$Prob(P|Q) = Prob(P) \tag{8}$$

Bayesian belief probability is calculated as follows,

$$Prob(P1 \ldots . Pn) = \prod_{i=1}^{n} Prob(Pi|Parents(Pi)) \tag{9}$$

In the context of Differential Privacy (DP), the parameter ε is known as the privacy cost, which controls the trade-off between data accuracy and privacy. A smaller ε value (e.g., 0.01, 0.1, 0.5, or 0.8) implies stronger privacy but introduces more noise. In our work, ε is adaptively chosen based on the packet size using a Bounded Laplace Mechanism. The noise injected output is defined as

$$X(D) = y(D) + noise \tag{10}$$

Where $y(D)$ is the actual data output and noise generated according to the Laplace Distribution. The standard deviation of the noise is derived as follows

$$\sigma(x) = \sqrt{P(x)},\ P(x) = 2l^2,\ \ l = \Delta y/\varepsilon \tag{11}$$

If the ε is small, then the larger noise will be added to the output.
The output variance is derived as,

$$P(x) = 2(\Delta y/\varepsilon)^2 = 2\Delta y^2/\varepsilon^2 \tag{12}$$

The corresponding standard deviation is derived as

$$\sigma(x) = \sqrt{P(x)} = \sqrt{\frac{2\Delta y^2}{\varepsilon^2}} = \sqrt{2}\Delta y/\varepsilon \tag{13}$$

Where, l is Laplace distribution and $\Delta y/\varepsilon$ is a noise, x represents probability density function.

3.3. Session key Generation and Lightweight Encryption

The Trusted Domain Authority (TDA) dynamically generates session keys based on the packet size, using the Chinese Remainder Theorem (CRT) and securely transmits them to the Cluster Head (CH). In the proposed framework, session keys are generated dynamically by the Trusted Domain Authority (TDA) using a combination of chaotic maps and the Chinese Remainder Theorem (CRT). Initially, a large pseudo-random sequence is generated using the Logistic Chaotic Map by carefully selecting initial conditions and a control parameter. From this sequence, the CRT randomly selects two co-prime moduli and two integer values to compute a unique solution that satisfies a system of modular congruences [18] [19]. CRT offers a solution to a set of simultaneous congruences with moduli that are coprime to each other. If (p, q) is a pairwise coprime integers such that $\gcd(p, q) = 1$ for $p \neq q$ (a, b) and are a pair of integers there exists a unique solution X such that

$$X \equiv a(mod\ P_1) \tag{14}$$

$$X \equiv b(mod\ P_2) \tag{15}$$

To securely transmit the session key to a designated CH, the TDA uses a PUF-derived symmetric key unique to that CH. To protect the session key during transmission, it is subsequently encrypted using the PRESENT lightweight cipher. The CH utilizes its hardware-intrinsic PUF to regenerate the key and decrypt the session key. This method guarantees resistance to device spoofing as well as confidentiality during key exchange. The data aggregated by the CH is XORed with the session key to ensure lightweight encryption.

Algorithm 3. Session Key Generation

Input: Control parameter r, Initial condition x_0, key length L.
Output: Binary key.
Begin
// Step 1: Create a pseudo-random sequence by applying the Logistic Chaotic Map.
$P_R \leftarrow$ Generate Chaotic Sequence (r, x_0)
// Step 2: Initialize empty key
key ← " "
// Step 3: Repeat until the key reaches desired length
While length(key) < L do
// Step 3a: Select two co-prime integers P_1 and P_2
$(P_1, P_2) \leftarrow$ SelectCoprimePair (P_R)
// Step 3b: Select two integers a and b such that $a < P_1$ and $b < P_2$.
$a \leftarrow$ RandomInt $(0, P_1 - 1)$
$b \leftarrow$ RandomInt $(0, P_2 - 1)$
// Step 3c: Apply Chinese Remainder Theorem to compute unique solution X.
$X \leftarrow$ CRT (a, b, P_1, P_2)
// Step 3d: Convert X to binary
bin_$X \leftarrow$ ToBinary (X)
// Step 3e: Append binary to the key.
key ← key || bin_X.
End While
// Step 4: Return generated key
Return key
End

Once a user is authenticated by the TDA, the request is forwarded to the corresponding gateway. To provide the requested service to the user, the gateway interacts with the server. The response is sent to the user in encrypted form. PRESENT is a lightweight block cipher with minimal area and memory footprints. It is a well-designed ultralightweight cipher optimized for resource-limited IoT systems. It encrypts data in 31 rounds and operates with a 64-bit block size and 80 or 128-bit key sizes. Each round comprises key addition, substitution via a 4-bit S-box, and a permutation operation [20]. These steps provide confusion and diffusion with minimal computation, making this cipher suitable for secure communication in IoT devices [21] [24].

Algorithm 4. PRESENT Cipher Operation

Input: Plaintext, Encryption key K.
Output: Ciphertext.
Begin
//Initialization
State ← $Plaintext$
//Perform 31 rounds of encryption
For round=1 to 31 do
roundKey ← Derive RoundKey(K, round)
state ← state ⊕ roundKey
If round < 31 then
    state ← sBoxLayer(state)
    state ← pLayer(state)
End If
End For
Ciphertext ← state

4. Experimental Results

The proposed framework is evaluated using the NS-3 network simulator. The system specifications and the simulation parameters are detailed in Table 2 and Table 3. Figure 4 shows the simulation of network. The threat resilience of the system is assessed by varying the number of malicious nodes in the network.

Table 1. Hardware and Software Configuration Used for Simulation

Software	Operating System	Ubuntu 14.04LTS
	Network simulator	NS3.26

Hardware	RAM	4GB
	Hard Disk	500GB

Table 2. Parameters and their description

Parameters	Description
Number of nodes	100 with 5% of attackers
Simulation area	$1000m * 1000m$
Maximum speed of node	$5\ m/s$
Mobility of node	random
Transmission range	$150\ m$
Initial Energy	$1\ J$
Number of flows	50

Node distribution	Random
Type of traffic	TCP, UDP
Packet transmission rate	1024 bytes/packet
Type of queue	Priority
Packet carrying duration	$1s$
Type of MAC	Ad hoc, Wi-Fi MAC
Propagation delay	Constant speed
Type of interface	Physical wireless
Capacity of forwarding	$2\ Mbps$

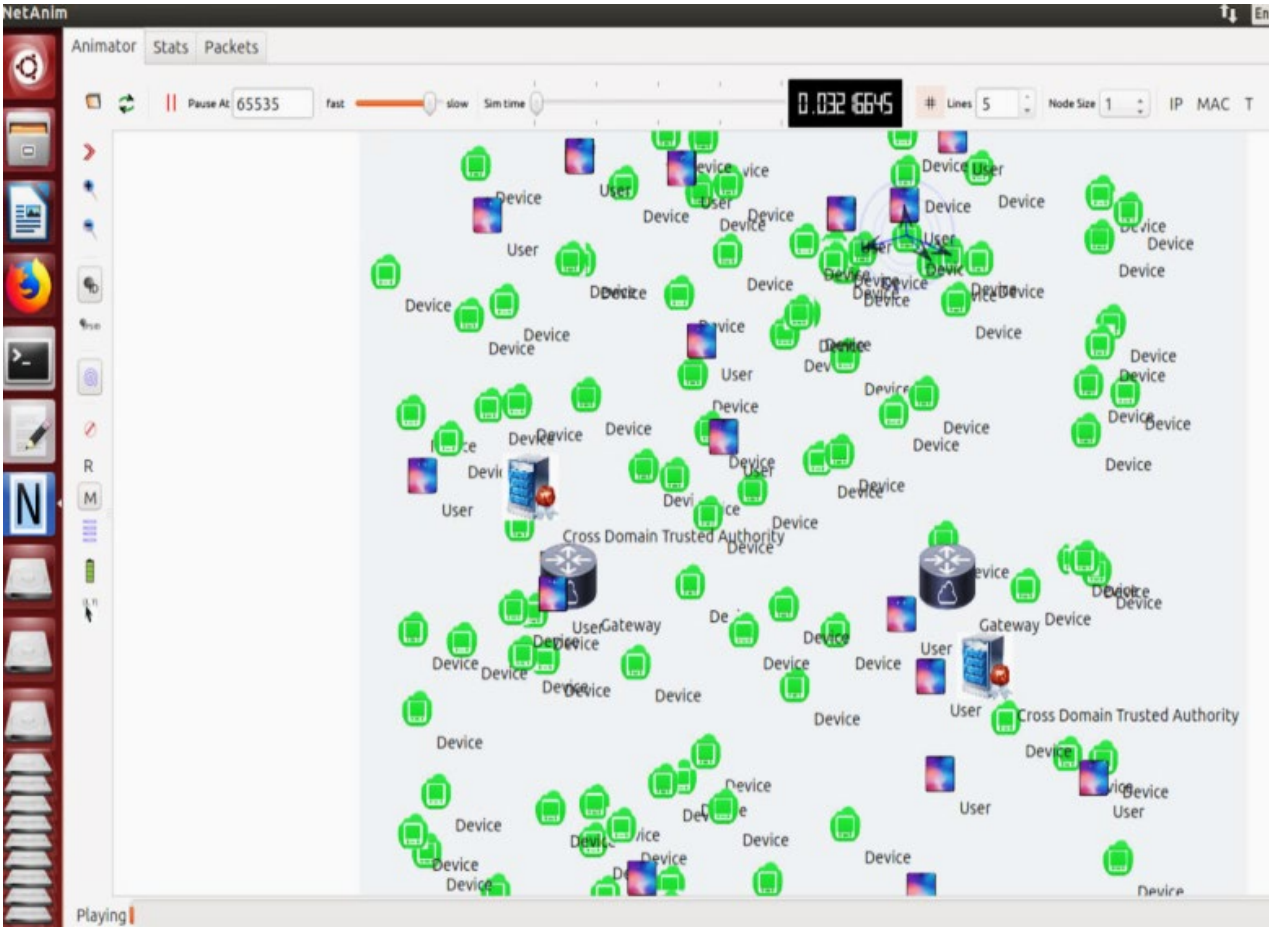

Figure 4. Deployment of IoT entities in the Simulation Environment

4.1. Comparative Study

The proposed system is evaluated in comparison with the ESMR protocol developed by Haseeb et al. Protean based authentication (PBA) developed by Sathyadevan et al. The malicious nodes are assumed to exhibit eavesdropping, spoofing, and deliberate packet dropping. The key performance metrics considered for the evaluation are Attack detection rate, throughput, energy consumption and end-to-end delay.These metrics offer a comprehensive picture of the system's capacity to sustain performance and security in hostile environments.

Attack Detection Rate

Attack detection rate measures a system's ability to detect malicious activities.

$$\alpha = \frac{no.of\ detected\ attacks}{total\ no.of\ attacks} \times 100\% \quad (16)$$

$$\alpha = \frac{TP}{TP+FN} \quad (17)$$

Where, α represents attack detection rate, TP represents True positives and TN represents True negatives. The BACS achieved higher rates than ESMR and PBA due to its multi-layered authentication, dynamic session key generation, and intelligent clustering. These mechanisms collectively ensure early identification and isolation of malicious nodes.

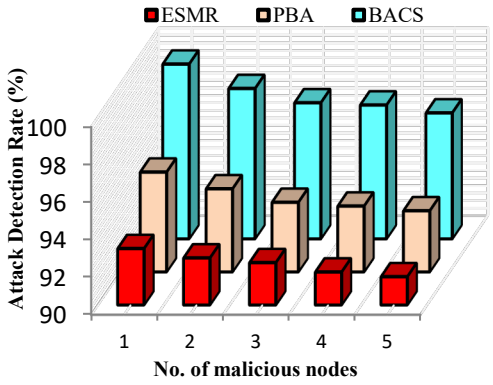

Figure 5. Comparison of Attack Detection Rate (%) under varying numbers of malicious nodes for ESMR, PBA, and the proposed BACS system.

End-to-End Delay

End-to-end delay refers to the total time taken for a data packet to travel from the source node to the destination node. Since the proposed method ensures the stable clustering and efficient cluster head selection mechanisms, it minimizes the frequency of re-clustering and minimizing retransmissions and route breaks. In contrast, existing systems lack such adaptive mechanisms and experience progressively increasing delay as the number of malicious nodes grows.

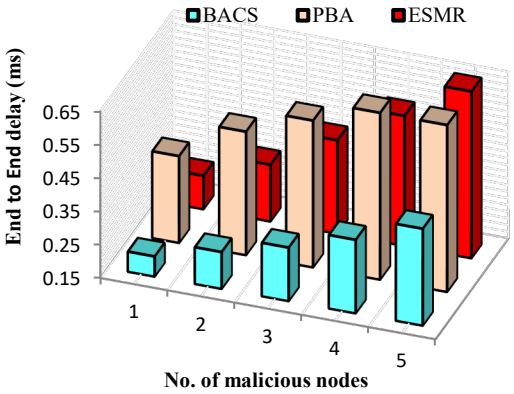

Figure 6. End-to-End Delay (ms) vs. Number of Malicious Nodes for ESMR, PBA, and the Proposed BACS System.

Energy consumption

Energy consumption refers to the amount of energy used by IoT devices during data transmission. It is calculated by subtracting the residual energy from the initial total energy of the node.

$$EC = \zeta - \mu$$

Where, EC represents energy consumption and ζ is a total amount of energy and μ is the remaining residual energy.

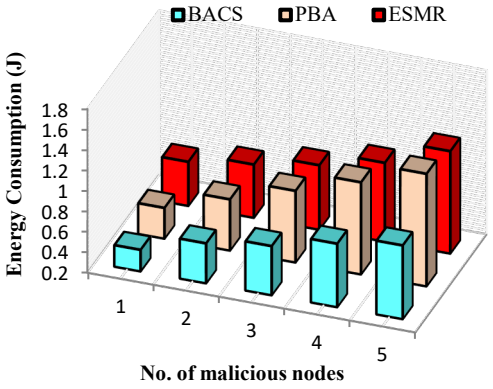

Figure 7. Energy Consumption vs. No. of nodes for ESMR, PBA, and the Proposed BACS System

Figure 7 shows the comparison of energy consumption between the proposed BACS system and existing methods across varying numbers of malicious nodes.

Throughput

Throughput is defined as the total number of packets successfully delivered per unit time. A higher throughput indicates superior system performance and effective data delivery. Figure 12 shows the throughput comparison between the proposed BACS framework and existing systems ESMR and PBA under varying numbers of malicious nodes.

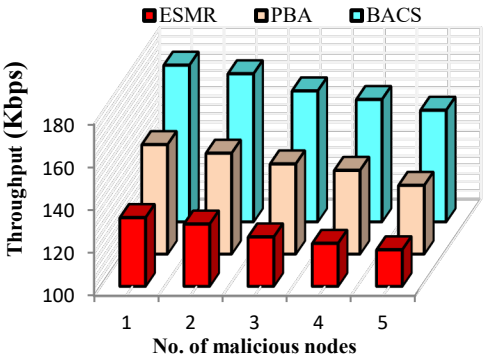

Figure 8. Throughput vs. No. of malicious nodes for ESMR, PBA, and the Proposed BACS System.

BACS achieves higher throughput due to stable CHs selected by OR-DQL. The packet losses are minimized by isolating malicious nodes and maintaining reliable

communication paths. On the other hand, ESMR and PBA experience lower throughput due to inadequate security measures and unstable CH selection, which increase packet losses.

5. Conclusion

This paper presents an integrated framework to implement both security and efficient clustering for IoT networks. The system utilizes blockchain technology to perform authentication, secure session keys to protect CH data, KNN-based classification for clustering, Optimal-Reward Deep Q-Learning for cluster head selection, and differential privacy to protect header information. The Trusted Domain Authority operates as an intrusion detection system by identifying compromised gateways and removing malicious nodes. Simulation results prove that BACS outperforms ESMR and PBA in various performance metrics. The BACS framework is currently validated only through simulations, and it considers only a limited set of attacks. Future research will focus on implementing BACS in real IoT testbeds, broader threat modeling, and advanced authentication with formal protocol verification.

References

[1] Wakili A, Bakkali S. Privacy-preserving security of IoT networks: A comparative analysis of methods and applications. Cyber Security and Applications. 2025;3.

[2] Rosa P, Souto A, Cecílio J. Light-SAE: A Lightweight Authentication Protocol for Large-Scale IoT Environments Made with Constrained Devices. IEEE Trans Netw Serv Manag. 2023;20(3):2428–2441

[3] Kumar A, Saha R, Conti M, Kumar G, Buchanan WJ, Kim TH. A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions. J Netw Comput Appl. 2022; 204.

[4] Zerrouki F, Ouchani S, Bouarfa H. PUF-based mutual authentication and session key establishment protocol for IoT devices. J Ambient Intell Human Comput. 2023;14:12575–12593.

[5] Saadati M, Mazinani SM, Khazaei AA, Chabok SJSM. Energy efficient clustering for dense wireless sensor network by applying Graph Neural Networks with coverage metrics. Ad Hoc Netw. 2024;156.

[6] Niakanlahiji A, Orlowski S, Vahid A, Jafarian JH. Toward practical defense against traffic analysis attacks on encrypted DNS traffic. Comput Secur. 2023;124.

[7] Mandal S, Bera B, Sutrala AK, Das AK, Choo KKR, Park Y. Certificateless Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment. IEEE Internet Things J. 2020;1(1):1–1.

[8] Sathyadevan S, Achuthan K, Doss R, Pan LP. Protean Authentication Scheme – A Time-bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments. IEEE Access. 2019;1:1–1.

[9] Haseeb K, Islam N, Almogren A, Din IU, Almajed HN, Guizani N. Secret sharing-based energy-aware and multi-hop routing protocol for IoT-based WSNs. IEEE Access. 2019;7:79980–79988.

[10] Fang L, Zhang H, Li M, Ge C, Liu L, Liu Z. A Secure and Fine-grained Scheme for Data Security in Industrial IoT Platforms for Smart City. IEEE Internet Things J. 2020;1:1–1.

[11] Luo X, Yin L, Li C, Wang C, Fang F, Zhu C, Tian Z. A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment. IEEE Access. 2020;1:1–1.

[12] Cui Z, Xue F, Zhang S, Cai X, Cao Y, Zhang W, Chen J. A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. IEEE Trans Serv Comput. 2020;1:1–1.

[13] Misra S, Mukherjee A, Roy A, Saurabh N, Rahulamathavan Y, Rajarajan M. Blockchain at the Edge: Performance of Resource-Constrained IoT Networks. IEEE Trans Parallel Distrib Syst. 2021;32(1):174–183.

[14] Chiang TH, Lo HY, Lin SD. A ranking-based KNN approach for multi-label classification. In: Proceedings of the Asian Conference on Machine Learning; 2012. Singapore: PMLR; 2012.

[15] Merah M, Aliouat Z, Mabed H. A Novel Cluster Head Selection Algorithm Based on Q-Learning for Internet of Things Networks. In: Proceedings of the 2024 International Conference on Telecommunications and Intelligent Systems (ICTIS); 2024; Djelfa, Algeria. p. 1–6.

[16] Zhu T, Ye D, Wang W, Zhou W, Yu PS. More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence. IEEE Trans Knowl Data Eng. 2022;34(6):2824–2843.

[17] Kadiyala R, Lakshmi Narayana CV, China Ramu S, Putta N, Pabboju SS, Ramana Reddy B. Trust-Aware Federated Learning with Differential Privacy for Secure AIoT in Critical Infrastructures. EAI Endorsed Trans IoT [Internet]. 2025 Dec. 2

[18] Rawool MPF. Chinese Remainder Theorem and its Applications. Goa: GOA University; 2024.

[19] Madhu GC, Perumal V. Encryption with automatic key generation and compression. In: Proceedings of the Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT); Aug. 2022; Kannur. p. 295–301.

[20] Bogdanov A, Knudsen L, Leander G, Paar C, Poschmann A, Robshaw MJ, Seurin Y, Vikkelsoe C. PRESENT: An ultra-lightweight block cipher. In: Proceedings of the Cryptographic Hardware and Embedded Systems (CHES); Sep. 10–13 2007; Vienna, Austria. Springer; 2007. p. 450–466.

[21] Madhu GC, Kumar PV. A survey and analysis of different lightweight block cipher techniques for resource-constrained devices. Int J Electron Secur Digit Forensics. 2022;14(1):96–110.

[22] Latah M, Toker L. Minimizing false positive rate for DoS attack detection: A hybrid SDN-based approach. ICT Express. 2020;6(2):125–127.

[23] Madhu, G.C., Vijayakumar, P. and Gao, X.Z. Resource constrained IOT environments: A survey. Journal of Advanced Research in Dynamical and Control Systems, 2017, 9(Special Issue 16), pp.445-457.

[24] J. J, K. T. Yadav CHT, M. Bharathi, M. G. C, V. K. Peroumal and R. Mitra. Software based performance evaluation of data encryption algorithms. In: Proceedings of the 2025 International Conference on Electronics, Computing, Communication and Control Technology (ICECCC); 2025; Bengaluru, India. Bengaluru: ICECCC; 2025. p. 1–5.

[25] G. C. Madhu, K. S. Reddy, M. M. Shabir, J. R. Kumar, G. P. Kumar and D. Srihari. Comparative analysis of energy aware routing techniques in WSN. In: Proceedings of the

2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE); IEEE; 2024. p. 926–929.

[26] S. Gnana Selvan, Jerith GG, C. Mahesh, Ravikumar S, Shaffi SS, S. Jagadeesh. A Trust Based Energy Efficient Routing Design Based on Hybrid Particle Swarm Optimization (HPSO) for Wireless Sensor Networks . EAI Endorsed Trans IoT [Internet]. 2025 Sep. 16 [cited 2025 Dec. 5];11