Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.060372

ARTICLE

HybridEdge: A Lightweight and Secure Hybrid Communication Protocol for the Edge-Enabled Internet of Things

Amjad Khan[1], **Rahim Khan**[1,*], **Fahad Alturise**[2,*] and **Tamim Alkhalifah**[3]

[1]Department of Computer Science, Abdul Wali Khan University, Mardan, 23200, Pakistan
[2]Department of Cybersecurity, College of Computer, Qassim University, Buraydah, Saudi Arabia
[3]Department of Computer Engineering, College of Computer, Qassim University, Buraydah, Saudi Arabia

*Corresponding Authors: Rahim Khan. Email: rahimkhan@awkum.edu.pk; Fahad Alturise. Email: falturise@qu.edu.sa

Received: 30 October 2024; Accepted: 14 January 2025; Published: 17 February 2025

ABSTRACT: The Internet of Things (IoT) and edge-assisted networking infrastructures are capable of bringing data processing and accessibility services locally at the respective edge rather than at a centralized module. These infrastructures are very effective in providing a fast response to the respective queries of the requesting modules, but their distributed nature has introduced other problems such as security and privacy. To address these problems, various security-assisted communication mechanisms have been developed to safeguard every active module, i.e., devices and edges, from every possible vulnerability in the IoT. However, these methodologies have neglected one of the critical issues, which is the prediction of fraudulent devices, i.e., adversaries, preferably as early as possible in the IoT. In this paper, a hybrid communication mechanism is presented where the Hidden Markov Model (HMM) predicts the legitimacy of the requesting device (both source and destination), and the Advanced Encryption Standard (AES) safeguards the reliability of the transmitted data over a shared communication medium, preferably through a secret shared key, i.e., λ, and timestamp information. A device becomes trusted if it has passed both evaluation levels, i.e., HMM and message decryption, within a stipulated time interval. The proposed hybrid, along with existing state-of-the-art approaches, has been simulated in the realistic environment of the IoT to verify the security measures. These evaluations were carried out in the presence of intruders capable of launching various attacks simultaneously, such as man-in-the-middle, device impersonations, and masquerading attacks. Moreover, the proposed approach has been proven to be more effective than existing state-of-the-art approaches due to its exceptional performance in communication, processing, and storage overheads, i.e., 13%, 19%, and 16%, respectively. Finally, the proposed hybrid approach is pruned against well-known security attacks in the IoT.

KEYWORDS: Internet of Things; information security; authentication; hidden Markov model; multimedia

1 Introduction

The Internet of Things (IoT) is an infrastructure of interconnected devices, i.e., things, to interact with physical phenomena via the embedded sensor(s) for capturing real-time data and sending it to the closest server or edge, where it is thoroughly examined for further processing. Edge-enabled IoT infrastructures were introduced to improve the response time of various queries regarding a particular phenomenon; that is possible only if multiple edge modules are incorporated in the IoT infrastructures instead of a single powerful centralized module [1,2]. Although the concept of multiple edges has drastically reduced the overall response time of individual queries that are generated by a legitimate device in the IoT because of the local availability of the respective data. As a wireless communication medium that is highly susceptible to unauthorized access is used for the transmission of captured data, preferably from the source device to the destination module in the IoT, it is highly likely that an intruder device may intercept ongoing messages or hijack an entire communication session [3]. In these scenarios, adversary modules pretend to be among the legitimate devices for the other party, which could compromise the whole IoT network. Therefore, effective methodologies could be developed to ensure reliable communication sessions among legitimate devices, particularly in the presence of adversaries. Cryptography-enabled communications are one of the most common ways to ensure reliable communication among member devices, preferably via shared wireless media [4]. In cryptography-enabled communication infrastructures, both devices, i.e., source and destination modules, use secret shared keys to convert plain text into cipher text and vice versa, thus making it hard (if not impossible) for intruder devices to read message contents in the IoT. In these systems, timely identification of the adversary module has become a cornerstone issue and is required to be addressed on a priority basis [5].

In the literature, mechanisms have been introduced to overcome this issue, i.e., devices' authentication and the prediction of intruders, particularly with existing technological infrastructures. An elliptic curve and secure certificate-enabled device's authentication scheme have been introduced to overcome the prevailing issue of establishing a trusted communication infrastructure, particularly with available resources in the smart healthcare environment of hospitals [6]. Additionally, this mechanism was developed for resource-constrained networks where devices have to rely on onboard batteries attached to the patient's body. Furthermore, the patient's data integrity is preserved through a sophisticated encryption scheme. A publish-subscribe-based device authentication scheme has been developed to ensure trusted communication sessions among IoT devices and edge modules [7]. This mechanism has adopted an empirically shared key concept, which is lightweight, instead of the heavy certificate-based schemes available in the literature. This mechanism not only protects against well-known intruder attacks, but it equally ensures non-repudiation as well. Likewise, a unique address and device identification-enabled methodology has been developed to protect the smart healthcare environment from fraudulent access and monitoring [8]. In this scheme, the session key concept has been utilized to preserve the anonymity of the intended source, particularly the user, and the destination module, i.e., the server, in the smart healthcare environment. To resolve the inherent weakness, that is, jamming attacks, of the existing radio frequency identification, an efficient mutual authentication scheme was developed where mutual keys among devices were constantly updated [9]. Apart from that, a self-adaptive nature was adopted that enables mutual devices to be consistent with the dynamic environment of IoT. A Chebyshev polynomial and session key-based authentication scheme were presented by Krishnasrija et al. [10] to safeguard next-generation networks from fraudulent access and well-known intruder attacks. Furthermore, a preregistration phase is required where secret information is shared among legitimate devices in the respective domain. Jan et al. [11] have developed a lightweight authentication scheme that is specifically designed for the Artificial Intelligence-enabled Internet of Things. In this approach, source and destination modules require four (4) phases to verify mutual authenticity in an active IoT. However, four phases mean four messages (two from each side), which is time-consuming and susceptible to man-in-the-middle attacks, especially if the adversary is equipped with a high-power computing device. Santhanalakshmi et al. [12] have developed an enhanced version of the conventional AES scheme by incorporating maximum diffusion properties in cipher text and key generation rounds. In short, numerous approaches have been introduced and developed to ensure that both parties, preferably those interested in communication, must belong to the class of legitimate devices. These approaches have underestimated an interesting phenomenon: the prediction of adversaries instead of detection. Secondly, existing authentication approaches were either developed for specialized communication infrastructures or domains, and their applicability in other domains is not trustworthy. Therefore, the development of a robust and effective methodology for the prediction of adversaries in a particular region is always appreciated by the research community in general and organizations in particular. A brief description of relevant papers and their respective limitations is presented in Table 1.

Table 1: Gaps and problems in the existing approaches

Scheme	Problem addressed	Limitations
Liu et al. [13]	Authentication	Couldn't address DoS attack
Gope et al. [14]	Security	Higher computational overhead
Hasan et al. [15]	Authentication and Communication	Higher processing cost overhead
Meddeb Makhlouf et al. [16]	Security and Authentication	Vulnerable to various attacks
Gupta et al. [17]	Authentication	Higher computational and Processing overhead
Hasan et al. [18]	Security	Vulnerable to various attacks
Al Rasheed et al. [1]	Authentication	Not applicable for Edge-enabled IoT

In this paper, we have developed a robust and hybrid model that is based on the Hidden Markov Chain Model and the Advanced Encryption Standard for the prediction of adversary modules in edge-enabled IoT networking infrastructures. Initially, every device, that is, ordinary modules and edges, participates in the offline phase, where secret keys, i.e., λ, are distributed among the legitimate devices by the concerned trusted authority. In this phase, the legitimacy of the requesting module is subjected to the provision of the medium access control (MAC) address that is required to generate its respective MaskID and is utilized during the communication phase. Secondly, during the communication phase, the requesting device must share valuable information such as MaskID and Maximum Transmission Delay ($\triangle$T) in the form of an encrypted message that is carried out via a secret shared key. The concerned edge module responds if and only if the authenticity of the requesting module is verified; that is performed through the utilization of the hidden Markov chain model. The main contributions of this paper are given below:

1. Development of a robust and effective technique or algorithm to predict the occurrence of the potential adversary module(s) in the coverage area of the respective edge module;
2. Establishment of secure packet transmission sessions among legitimate modules and respective edges in the presence of adversaries in the IoT;
3. A methodology to separate legitimate modules from adversaries in the operational networks without compromising on their performance metrics.

The remaining manuscript is organized as follows: In the following section Section 2, we have focused on how the Hidden Markov Chain-enabled prediction model is formed and utilized to separate legitimate modules from intruder devices. In Section 3, a comprehensive analytical discussion is provided where the vulnerability of the proposed scheme against well-known intruder attacks has been thoroughly evaluated and discussed. Moreover, simulation results of the proposed and existing schemes with supportive graphical and tabular representations are presented in the next section. Finally, concluding remarks and future directions are given in Section 5.

2 Proposed Hybrid Prediction Model for the Edge-Enabled Internet of Things

Due to its overwhelming properties, the edge-enabled Internet of Things has been considered a cornerstone in the next generation of networking infrastructures, whether traditional networks or resource constraints. In both scenarios, a shared communication medium that is highly susceptible to fraudulent access is used where it is highly likely that an ongoing or newly established communication session could be compromised. Secondly, the authenticity of the respective edge module should be verified by the requesting module through a sophisticated procedure, which initiates the transmission of actual data only if security measures are intact. Thirdly, the edge module should follow certain cryptography-enabled techniques, i.e., Hidden Markov Chain and AES in this case, to separate fraudulent requests from legitimate ones in its coverage area or domain. In both cases, an adversary module could pretend to be a legitimate device; that is possible only if one of these modules is compromised. To safeguard against these threats, a hybrid prediction model is presented to enable the establishment of secure communication sessions among trusted (authenticated) modules, and message contents are secured through an AES-enabled encryption scheme. The proposed model has two distinct phases: (i) offline and (ii) online. A detailed description of these phases is provided in the following Sections 2.1 and 2.2.

2.1 Offline Phase of the Proposed Hybrid Model

In the offline phase, the Trusted Authority (TA) generates a message and broadcasts it to gather information from the legitimate modules, that is, both ordinary devices and edge devices, that reside in its coverage area. Moreover, we have assumed that activities related to the offline phase are carried out in a secure environment that is free from fraudulent or unauthorized access and reporting. Therefore, message contents should be in a readable format, i.e., plain text, for every module in the edge-enabled IoT. In response to this message, every device updates its contents and provides MAC address information in plain text form. The updated message is sent to the TA, which computes the MaskIDs of the respective MAC addresses and shares them back with the devices in the edge-enabled IoT. Secondly, TA shares a secret key with the legitimate modules, which is both an ordinary device and an edge, along with a list of legitimate devices and edge(s) MaskIDs instead of the original MAC addresses. The TA generates MaskIDs for every device and server module, which are directly correlated to the original MAC address in IoT. For this purpose, a 48-bit address, i.e., 01-A2-99-FB-75-C9 in hexadecimal format, is selected, and the exclusive OR operation is carried out with the device's MAC address. The resultant address, i.e., 48 bits, is the required MaskID that is shared with the respective device in IoT.

2.2 Authentication Phase of the Proposed Hybrid Model

In the authentication phase, every module, that is, both the source (requesting device) and the destination (edge), should be verified before triggering the actual communication session, as it is highly likely that both devices could be adversaries. For this purpose, the source module, which is interested in initiating a proper communication session, generates a message where its MaskID along with interest in starting a session is appended and encrypts the message contents with its secret key, i.e., λ_i, to protect it from fraudulent devices or adversaries in the edge-enabled IoT. The encrypted message is sent to the intended destination module, which is Edge in this case. Additionally, every device appends a time stamp along with the MaskID to the message contents, which is very fruitful in various attacks, such as reply or perfect forward. This timestamp is not only helpful in the prevention of various attacks; it is equally important to differentiate a compromised, verified device in the edge-enabled IoT as well. Now, if this message is intercepted by the legitimate module, i.e., edge, then it converts the cipher text into the proper plain text format using its secret key λ. The respective MaskID of the requesting device, which was appended to the message contents, was matched against the MaskIDs of the legitimate modules, which are stored in the form of a list. If a match is encountered, then verification of the requesting device is confirmed, as both the secret key and MaskID are shared in the offline phase. The respective edge module modifies the contents of the message, especially MaskID, according to its own information and encrypts it with the secret key λ. The updated encrypted message is sent to the concerned module, where it is converted into plain text via a secret shared key. The requesting module extracts the message contents, preferably the MaskID of the intended destination module, and searches for them within the list. In the case of matching MaskID, the authenticity of the destination module is confirmed as both secret key λ and MaskIDs were shared in the offline phase, which is assumed to be safe from fraudulent access. Both modules have confirmed the authenticity of each other and could start the transmission of actual data, preferably encrypted through a 128-bit secret shared key, λ.

Alternatively, if the encrypted message of the source module is intercepted by an adversary that is deployed in the vicinity of the device and tries to pretend to be a legitimate edge module. The initial task of the concerned adversary module is to read the contents of the message; that is possible only if this device, i.e., adversary A_k, has the secret shared key λ. As λ is shared in the offline phase, which is far beyond the adversary's reach, it will therefore adopt brute force or head-and-tail mechanisms, which are computationally expensive and time-consuming, to convert encrypted messages into proper plain text or readable form. Secondly, these mechanisms require high-power processing devices to complete the conversion task within a defined time frame. However, IoT devices have resource constraints, and thus cracking a 128-bit AES-enabled key is not possible with the available processing powers of these devices. Secondly, if the adversary module generates its own message, it will require the secret shared key λ, which is not available. If the adversary transmits its own generated message in plain text form, then it is an indication to the legitimate requesting device that it is not from the authentic module.

The respective edge module is likely to be deployed such that it falls within the coverage area of the maximum ordinary device (if not all), and every module can communicate directly with it in the edge-enabled IoT. In the proposed prediction mechanism, the edge module has the built-in capacity to extensively evaluate incoming authentication requests from legitimate modules. For this purpose, numerous metrics have been used, such as a request through an encrypted message via its secret share key λ, probably equal delivery time of packet $\triangle$T, MaskID, the current timestamp, and the expected response time to a particular message. In the initial stages, the aforementioned authentication approach has been utilized to separate legitimate modules from adversaries. However, with time, the respective edge module has sufficient data about every legitimate device and is in a position to predict with the highest level of confidence whether a requesting module is legitimate or an adversary. For this purpose, the edge module adopts the well-known prediction mechanism, which is the hidden Markov chain model. To verify the authenticity of the requesting module, i.e., both legitimate C_i and adversary A_k, through a defined set of parameters that are shared with the respective edge module through a message request. The concerned edge module divides legitimate devices into the following groups:

1. Regular Modules: those continuously requesting, preferably after a defined interval of time, for authentication and the establishment of communication sessions. These modules have taken part in the offline phase and have a secret key λ and a verifiable MaskID, along with a predictable requesting process.
2. Event-based Modules: Request authentication regularly when a particular event has been triggered. These modules send a verification and session establishment request when a respective event occurs. That is, a device embedded with a smoke sensor sends an authentication and session establishment request when the smoke has been detected, such as cigarette smoking.

When the edge module receives an authentication and session establishment request from a member module in the IoT, it verifies its authenticity through the Hidden Markov Chain Model by passing various parameters such as the secret key λ, MaskID, △T, time stamp, and module type as described in the Fig. 1 After passing parameters, if the expected value of the requesting module is greater than the defined threshold value of the hidden Markov chain model, that is 0.1%, it is assumed to be a legitimate module and permitted to establish a proper communication session. However, if the computed value is less than the threshold value, then it indicates illegal or out-of-the-way activity and could be a potential intruder attack. Thus, the respective edge module blacklists the requesting module and includes its credentials in the class of potential adversaries, and at the same time, it informs member devices about potential security threats in the coverage area.

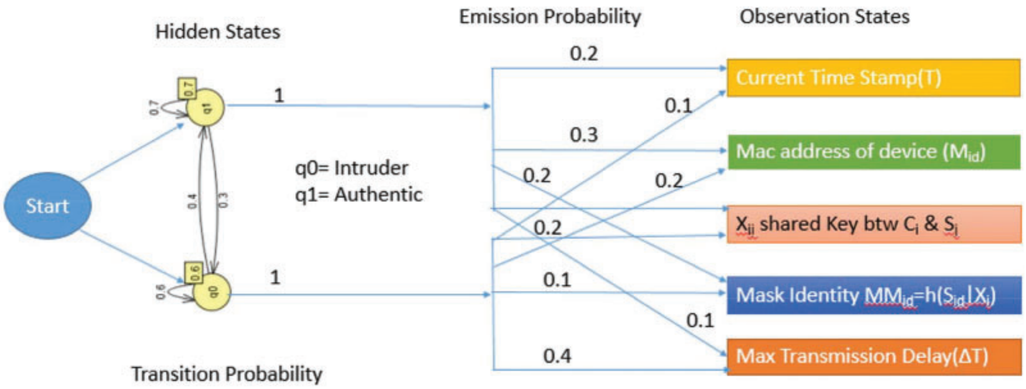

Figure 1: A generalized structure of the utilization of the hidden markov chain model in the proposed prediction technique

Let's assume that the respective IoT infrastructure has a total of N-member devices, which is based on a statistical analysis of the offline phase. Additionally, at time T_i, if n represents the approximate number of devices that make a request for verification and onward triggering of the actual communication session, and m represents devices that are legitimately not interested in communication, Furthermore, among these devices, P percent have initiated a verification request to the respective edge module at time T_i. Similarly, p percent of those legitimate devices, that didn't send a verification request at time T_i, have sent a session initiation request at time T_{i+1}. Initially, the respective edge module needs to find out how many devices will be interested in initiating a proper communication session in the next time stamp. As per the assumption, p percent (n) and q percent (m) will send verification requests at time T_{i+1}. Thus, the approximate verification requests, which are likely to be sent in the next timestamp, are as given in Eq. (1).

$$b_1 = (p * n) + (q * m) \tag{1}$$

Similarly, the approximate number of devices that are not interested in sending a verification request in the next timestamp is as given in Eq. (2).

$$b_1 = (1 - p * n) + (1 - q * m) \tag{2}$$

This system of the underlined equations could be represented by Mx = b, as given below in Eqs. (3)–(5), respectively.

$$M = \begin{pmatrix} p & q \\ 1-p & 1-q \end{pmatrix} \tag{3}$$

where p and q represent probabilistic values of whether the legitimate module is interested or not in initiating a reliable communication session in the next time stamp, respectively.

$$x = \begin{pmatrix} n \\ m \end{pmatrix} \tag{4}$$

where n and m are used to describe requesting and not-requesting parties in the edge-enabled IoT, respectively.

$$b = \begin{pmatrix} Interested \\ Not\,Interested \end{pmatrix} \tag{5}$$

The expected probability of a legitimate module making a request for proper communication is based on the value computed through Eq. (6) as given below. It is important to note that the prediction accuracy of the respective edge module is subjected to the approximate values of parameters p and q, respectively. Additionally, the hidden Markov chain model is an ideal approach in scenarios where it is possible that a legitimate device or module has been compromised, which occurs when a device gets captured and controlled by the adversary module. In these circumstances, the intruder device pretends to be the respective legitimate device; however, the proposed Hidden Markov Chain-enabled authentication scheme enables the respective edge module to refrain such devices from granting permission to initiate a proper communication session. Secondly, the proposed approach forces every module to clear its log file, preferably after the communication session is ended, which further safeguards the system or module from fraudulent access and use.

$$b = \begin{pmatrix} p * n + q * m \\ 1 - p * n + 1 - q * m \end{pmatrix} \tag{6}$$

A requesting module is granted permission to initiate a proper communication session if the computed value of the Eq. (6) is greater than the defined threshold value. Alternatively, a request is denied if the value is less than or equal to the threshold value. Thus, the proposed system is not only secured through a 128-bit enabled secret key, but it is equally applicable to separate legitimate requests or devices from false ones.

2.3 Device and Server Modules Architecture

During the simulation, every device is deployed within the coverage area, to ensure direct communication, of at least one server module, preferably the one that has the maximum RSSI value, in IoT. Secondly, devices communicate directly with the respective server module, preferably the one that resides in the coverage area. A generalized structure of the proposed authentication approach for the IoT infrastructure is presented in Fig. 2 where devices interact directly with the environment through embedded sensors to capture the required information after defined time intervals, i.e., sampling rate ranges from 5 to 150 ms. Secondly, every communication session is protected through an HMM and AES-enabled security scheme. Every message is encrypted with a 128-bit AES along with other important metrics in the payload of a packet. Thirdly, the respective authentication process is mutual, i.e., the device and server module verify the authenticity of each other through a sophisticated procedure, that is HMM and AES along with time stamp information. Moreover, an adversary or intruder module could be anywhere, a device (where a device impersonation attack is triggered) or a server (where server impersonation attack is triggered) module in IoT. Algorithm for the proposed methodology is presented in Algorithm 1.

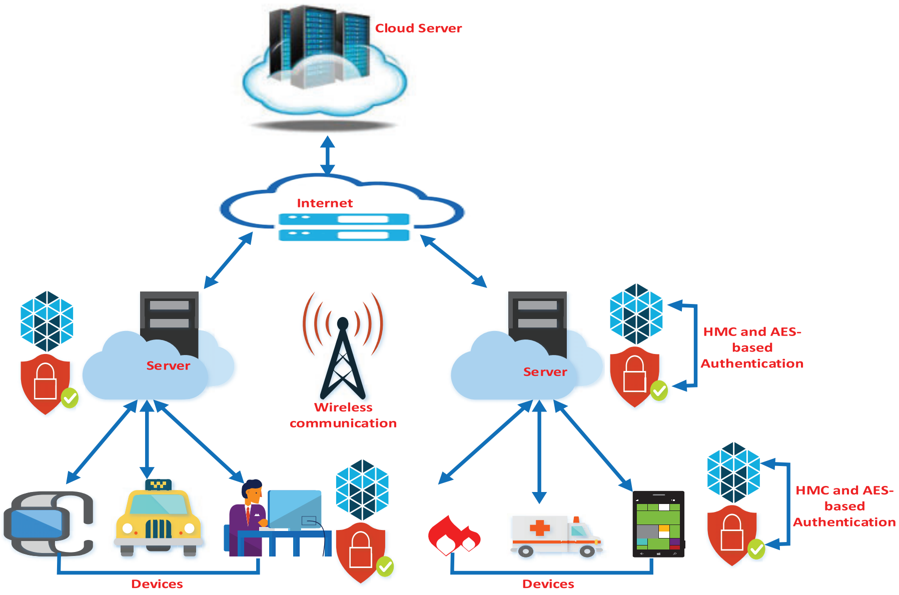

Figure 2: Generalized architecture of the proposed authentication scheme in the Internet of Things

Algorithm 1: Proposed hybrid authentication algorithm for the edge-enabled Internet of Things

```
Require: Requesting Modules $C_i \& A_k$
Ensure: Permitted or Not Permitted $(C_i)$
Class – member ← Zero
$\delta$ ← value
$Adversary$ ← Zero
$N$ ← Module in IoT
for every $C_i \rightarrow n \in IoT$ do
    $msg_i = MaskID_i$
    $msg_i$ = AES($msg_i$)
    Transmit $msg_i$
    if $MaskID(C_i) \in Class - member$ ) & HMC-Value > $\delta$ then
        $C_i$ Permitted
    elseif $MaskID(C_i) \notin Class - member$) then
        $C_i$ Not Permitted
        $C_i$ is Black-listed
    elseif $MaskID(C_i) \in Class - member$) & HMC-Value <= $\delta$ then
        $C_i$ Not Permitted
        $C_i$ could be an Adversary
        Investigate Further
    end if
end for
return Permitted or Not
```

2.4 Proposed Hybrid Authentication Algorithm for the Edge-Enabled Internet of Things

This subsection is dedicated to the crucial part of the proposed hybrid authentication approach for the edge-enabled IoT, that is the algorithm, and is defined as the set of rules required to be followed for achieving the expected result in the underlined domain. $Class - member$ is used to store MaskIDs of the legitimate module, particularly those taking part in the offline phase, in the edge-enabled IoT, whereas the $Adversary$ class is used to keep a record of the potential intruder module in the edge-enabled IoT, where "i" represents the indexing value of a device such as C_1 describes device one in IoT. HMC-value is the defined threshold value computed using Eq. (6) to separate legitimate requests from the fraudulent ones in the operational IoT.

3 Security Analysis (Informal) of the Proposed Hybrid Prediction Approach for the Internet of Things

Generally, a newly developed security algorithm must be thoroughly examined through well-known intruder attacks to confirm whether it has any security flaws or not when implemented in the real working environment of the IoT. For this purpose, the vulnerabilities of the proposed approach are extensively exposed and evaluated in the presence of one or more adversary modules. Initially, the newly developed scheme is tested against every possible attack on an individual basis, and it should be pruned against these attacks in the IoT. In the next stage, multiple intruder attacks are triggered simultaneously to verify its susceptibility to these attacks in the open environment of the IoT. In similar fashion, the proposed prediction algorithm is tested against various possible intruder attacks, such as man-in-the-middle, reply attacks, and device impersonation attacks. A detailed discussion of these attacks is given below.

3.1 Masquerading Attack in the IoT

Impersonation attacks are defined as the mechanism adopted by the respective intruder module A_k to pretend to be a legitimate module to another party and try to steal or extract valuable information from the IoT. In this case, the hacker tries to convince the receiving module that it is a legitimate module and trick the module into sharing valuable data about a particular phenomenon. An attacker can deceive both a legitimate device and an edge module by pretending to be a trusted edge and device, respectively.

3.1.1 Legitimate Module Impersonation

Let's assume that an adversary is interested in stealing captured data from the respective edge module in the IoT. The Adversary module is required to generate a cipher text message where its MaskID is embedded along with timestamp information. However, the proposed hybrid prediction scheme bounds every legitimate module to encrypt a message via a secret key that is shared in the offline phase and which was assumed to be a no-entry zone for the adversaries. Secondly, MaskID is allocated to every trusted module and is required to be embedded in the encrypted message. Both of these parameters are far beyond the access of the adversary module, and thus if it tries to impersonate one of the legitimate modules, then MaskID and λ of the respective module are required. Secondly, if the adversary module tries to convert one of the intercepted messages, then it is very hard as far as the security of the 128-bit AES scheme is concerned. Thus, the proposed prediction approach is pruned against the impersonation of the legitimate module.

3.1.2 Edge Module Impersonation

Likewise, if an adversary tries to pretend to be a legitimate edge module, then all it needs is the MaskID and secret key λ of the respective device. Secondly, as every module in the proposed setup has a list of the MaskIDs of the edge module(s), messages intercepted from those modules, for which MaskIDs are not known, are simply ignored. In the proposed approach, it is very hard for the adversary to pretend to be a legitimate edge module, as it can't break a 128-bit secret key with the available resources. Secondly, if it somehow converts the cipher text message into equivalent plain text, then it will be identified as an adversary because it is very hard to meet other parameters of the Hidden Markov Chain Model such as timestamp, average propagation time, and response time, respectively, in the IoT. Thus, the proposed prediction approach is pruned against edge impersonation attacks triggered by the adversary modules.

3.2 Eavesdropping Attack

In this attack, an intruder module intercepts every message, particularly those transmitted via a non-secured and shared medium, destined for a legitimate module, and updates or discards it accordingly. However, every message that is either related to authentication or actual data is encrypted with a secret shared key λ, a 128-bit AES key, and, thus, is protected against eavesdropping attacks. Even though these messages are transmitted over shared and unsecured channels in edge-enabled IoTs. Secondly, 128-bit AES is among the strong keys and requires extensive computational and processing power to break it through continuous utilization of brute force or head-and-tail methods; however, it requires extensive efforts and time resources. As messages are transmitted in encrypted form, the proposed approach is to protect against eavesdropping attacks in the IoT domain.

3.3 Man-in-the-Middle Attack

In this type of attack, an intruder module tries to hijack an ongoing communication session among legitimate modules in the IoT. In this case, the perpetrator module may pretend to be legitimate (like an impersonation attack) or try to steal information from unprotected messages (like eavesdropping). The proposed scheme is pruned against mimicking the policy of the respective intruder device, as every message is properly encrypted through a 128-bit secret key along with other important parameters that are required by the Hidden Markov Chain Model to separate legitimate modules from the adversaries in the IoT. Secondly, it is not vulnerable to the second methodology adopted by the intruder module as messages are transmitted in encrypted form, which is beyond the processing capabilities of the resource-constrained devices.

3.4 Denial of Service Attack

In a denial-of-service attack, a perpetrator module tries to make the resource of the underlined network or domain unavailable to its users, which are legitimate devices in this case. For this purpose, perpetrator modules adopt different mechanisms, such as sending multiple requests simultaneously to the respective edge module. However, in the proposed setup, the concerned edge module processes only those messages that are encrypted through the secret shared key. The perpetrator modules haven't attended the offline phase, and thus, these modules don't have the required encryption key. Therefore, messages sent by these modules are ignored by the respective edge modules as they are not encrypted with a proper key, and, thus, it is protected against denial-of-service attacks in the IoT.

3.5 Brute-Force Attack

In brute-force attacks, perpetrator modules try to break the security key that is used to encrypt the transmitted message via different methodologies. However, the proposed prediction mechanism utilizes a 128-bit AES secret key, which is very hard to guess. Additionally, perpetrator modules must have sophisticated and high-power computing resources to break the security key, but 128-bit is very strong and would require excessive time (in years) and exceptional computational power to reach a conclusion, i.e., the required secret key. Thus, the proposed hybrid prediction scheme is pruned against brute-force attacks in traditional networks in general and IoT in particular. A detailed analysis of the proposed prediction security measure and its susceptibility to various perpetrator attacks is presented in the Table 2 given below.

Table 2: Comparison in terms of security features

Security metric	Liu (2016)	Hasan (2013)	Makhlouf (2019)	Gupta (2019)	Abdelshafy (2014)	Proposed scheme
Masquerading attack client	✓	✓	✓	✓	✓	✓
Anonymity traceability	✓	✓	✓	✓	✓	✓
Masquerading attack device	✓	✓	✓	✓	✓	✓
Replay attack	✓	✓	✓	✓	×	✓
Masquerading attack edge module	×	✓	×	×	✓	✓
Eavesdropping attack	×	×	✓	✓	×	✓
Brute-force attack	✓	✓	✓	✓	×	✓
Denial of service attack	✓	×	✓	✓	✓	✓
Man-in the middle attack	✓	×	×	✓	×	✓

4 Performance Evaluation of the Proposed Hybrid Secure Communication

This section presents a comprehensive evaluation analysis of the proposed, i.e., hidden Markov chain and AES-enabled prediction technique, and existing security algorithm in terms of numerous important IoT authentication performance metrics such as energy consumption, response time, average transmission delay, computation power required, processing, and storage overhead. For this purpose, these algorithms were implemented in OMNET++ an open-source software available for simulation, and these implementations are executable on Core i5 sixth generation and onward processing power computers or laptops. Additionally, we have assumed that the processing, communication, and storage power of the member modules in the proposed edge-enabled IoT is an exact copy of the Wasp-mote boards with embedded sensors, which are limited in terms of various embedded resources. Numerous parameters or resources used to set up the simulation environment for both the proposed edge-enabled communication and the existing state-of-the-art approach are presented in Table 3 as given below.

Table 3: Brief description of simulation parameters used in the edge-enabled IoT

Parameters	Approximate value
Coverage area	900 m × 900 m
Devices (active)	500–2000
Edge modules	1
Onboard battery power (E_i)	6600 and 52,000 mAh
Residual power (E_r)	Device oriented
Power needed for transmission (P_{T_x})	91.4 mW
Channel-Delay (Ch_{delay})	10 ms
Power needed for receiving (P_{R_x})	59.1 mW
Power consumption (Idle Mode)	15.4 μW

(Continued)

Table 3 (continued)

Parameters	Approximate value
Transceiver's power (Idle) (T_i)	1 mW
Transmission range (T_r)	500 m
Packet size (Actual Data)	128 bytes
Encryption	128-Bit AES
Module's sampling rate	30–150 ms
Topology	Static and Random
Traffic type	CBR and UDP

Performance analysis of the proposed and existing algorithms for edge-enabled IoT networks is presented in the following subsections.

4.1 Computational Cost Overhead of Additional Parameters

Computational cost is among the crucial evaluation metrics in traditional networking infrastructures in general and edge-enabled IoT in particular. An authentication algorithm with the minimum possible computational cost is considered an ideal approach for resource-constrained networks; however, this algorithm shouldn't compromise on other performance metrics. For this purpose, a comparative evaluation analysis of the proposed hybrid and existing state-of-the-art algorithms is depicted in Table 4, where the computational cost performance testing metric is used. The proposed hybrid authentication schemes' Hash function and exclusive OR operation values are based on the number of these metrics integrated with the conventional AES scheme to enhance its security a bit further. The proposed hybrid authentication scheme has successfully attained the minimum possible level of computational overhead among other algorithms. As the proposed algorithm has used a 128-bit AES scheme to convert plain text messages, i.e., those generated by legitimate modules, into equivalent cipher text, it requires the least possible values of the hash function and exclusive ORs, as depicted in Table 4. This minimum value of the computational cost makes it the most prominent scheme for edge-enabled IoTs.

Table 4: Evaluation of the computational cost overhead

Algorithms	User/Client	Modules C_i	Edge/Server S_j	Total cost
Proposed Hybrid Algo	–	$4T_h + 4T_{XOR}$	$4T_h + 4T_{XOR}$	$8T_h + 8T_{XOR}$
[17]	$7T_h + 4T_{XOR}$	$4T_h + 4T_{XOR}$	$5T_h + 3T_{XOR}$	$16T_h + 11T_{XOR}$
[15]	$2T_{PA} + 2T_{PM}$	$2T_{E/D} + 2T_{PRNG}$	$3T_{TS} + 1T_{TKNG}$	
[19]	$7T_h + 4T_{XOR}$	$4T_h + 4T_{XOR}$	$5T_h + 3T_{XOR}$	$16T_h + 11T_{XOR}$
[14]	$3T_h + T_{XOR}$	–	$9T_h + 4T_{XOR}$	$12T_h + 5T_{XOR}$
[16]	–	$2T_h + 6T_{XOR}$	$7T_h + 7T_{XOR}$	$9T_h + 13T_{XOR}$
[18]	$2T_h + 6T_{XOR}$	$2T_h + 5T_{XOR}$	$3T_h + 3T_{XOR}$	$7T_h + 14T_{XOR}$
[20]	$5T_h + 5T_{XOR}$	$2T_h + 1T_{XOR}$	$2T_h + 6T_{XOR}$	$6t_h + 11T_{XOR}$
[13]	$3T_h + 3T_{XOR}$	–	$4T_h + 12T_{XOR}$	$7T_h + 19T_{XOR}$

Additionally, these algorithms were extensively compared in terms of computational cost for both legitimate and edge modules, respectively, as depicted in Figs. 3 and 4, where the proposed algorithm has shown exceptional performance. These algorithms were tested using different scalability ratios of the underlined IoT, that is, from three hundred to 2100 modules. Secondly, these experiments were carried out in the presence of various adversary modules and through the continuous launching of multiple intruder attacks simultaneously in the IoT.

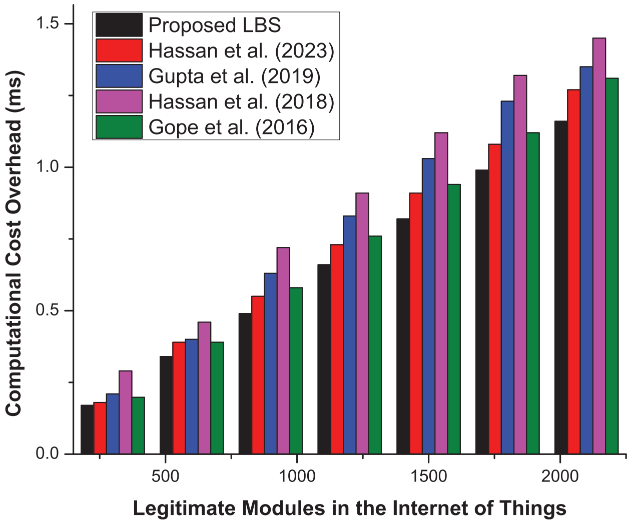

Figure 3: Comparative evaluation of the proposed hybrid and existing state of the art algorithms (Module side)

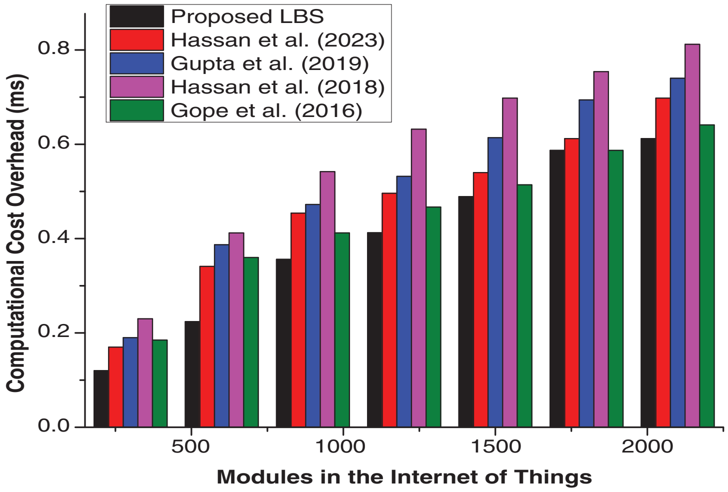

Figure 4: Graphical depiction of the comparative evaluation of the proposed hybrid and existing state of the art algorithms (Edge side)

4.2 Communication Cost Overhead

Communication cost overhead is among the crucial performance evaluation metrics as it is related to the effective utilization of the most important networking resource, i.e., bandwidth, which must be utilized efficiently in traditional networks in general and IoT in particular. In Table 5, an extensive evaluation of the proposed hybrid and existing state-of-the-art algorithms is presented in the Table 5 particularly in terms of messages and bits communicated in the different phases. The proposed hybrid approach has the minimum possible communication overhead, i.e., 640 bits, as compared to the existing algorithms. Secondly, in the proposed hybrid algorithm, two messages are required in the offline phase, which is a one-time process, to get the secret key and MaskID. In the authentication phase, two messages are enough to separate the legitimate module from the adversaries in the IoT. Additionally, if we exclude the offline phase from the proposed hybrid algorithm, then its communication cost is much lower as compared to the existing approaches.

Table 5: Comparison of the communication cost overhead

Algorithms	No. of messages	No. of bits
Proposed Hybrid Algo	4	640
[13]	4	4672
[14]	4	3184
[15]	6	672
[16]	5	6144
[17]	5	3038
[18]	6	32,000
[20]	5	24,546
[13]	6	30,620

Apart from the tabular representation of the proposed and existing algorithms, a comparative study (particularly graphical results) of these algorithms in terms of communication cost overhead is carried out as well. From Fig. 5, we have observed that the proposed hybrid algorithm has achieved an overall authentication process with the minimum possible end-to-end delay metric and overall bits transmitted in the IoT.

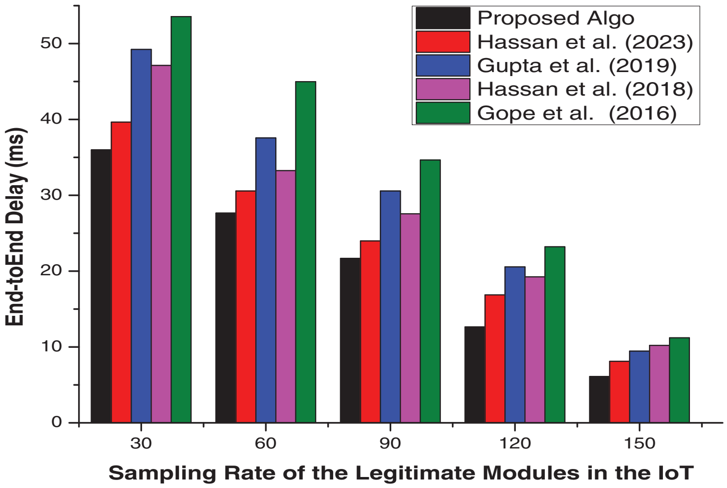

Figure 5: Graphical depiction of the comparative evaluation, particularly in terms of communication cost, of the proposed hybrid and existing state of the art algorithms

4.3 Storage or Memory Overhead

Generally, in resource-limited networks such as IoT, the onboard memory of a module is crucial as it has a direct correlation to the smooth functionality of the underlined device. Therefore, we have depicted an extensive summary of the proposed hybrid and existing approaches to storage overheads in Table 6. In the proposed setup, a module should keep a list of the legitimate devices, i.e., MaskIDs, along with its secret key, λ, that is shared in the offline phase. It is important to note that some of the existing approaches, i.e., Gope et al. [21], either don't use storage or, if they do, are very low as compared to the proposed scheme. However, these algorithms are very expensive, particularly in terms of computational and communication overheads. Furthermore, a graphical representation of the proposed and existing algorithms' storage overhead is shown in Fig. 6, where the former approach outperforms later approaches in the IoT.

Table 6: Comparison of the storage cost overhead

Algorithms	Modules	Server gateway
Proposed hybrid approach	$MasID_j\lambda_i$	$MasID_i\lambda_j$
[17]	$e_j + f_j + x_j + MI_u + MGID_i$	$MSID_j + Z_j + x_i$
[14]	–	$x_{id} + Ts_{ug} + \omega + K_{ug} + Ts_{ug_{new}} + Sn_{id_i}^{new} + k_{gs_i}^{new}$
[13]	$ID_i + \lambda_i + ID_G + \lambda_G$	$\mathrm{n}ID_i + \lambda_i\,\mathrm{m} + ID_G + \lambda_G$
[15]	Q_{AG} (server) + μ_i	Q_{AG}(device) + μ_i
[16]	—	$PK_{RSU} + PK_{TA} + V_i + K_{vi} + ID_{vi}$

Where i, and j represent indexing terms for devices and server or edge modules in IoT, respectively. $\lambda\mu$ represent the secret and session keys, respectively. Likewise, $x_i, f_i, \&e_i$ store intermediate results. $MSID_j and MSID_i$ represents the Masked Identity of jth Sensing device and ith mobile terminal, respectively. $Ts_{ug}\&\omega$ are the transaction sequence number (maintain both U and GW) and Secret key of the gateway, respectively. K_{ug} is the shared key between U and GW, and S_n sensor. Q_{AG} represent public keys of the aggregator point of the server and device, respectively. Finally, $PK_{RSU}\&PK_{TA}$ represent Public keys of Road Side Unit and Trusted Authority, respectively. V_i, K_{vi}, and ID_{vi1} represent sender vehicle, permanent key, and unique identity, respectively.

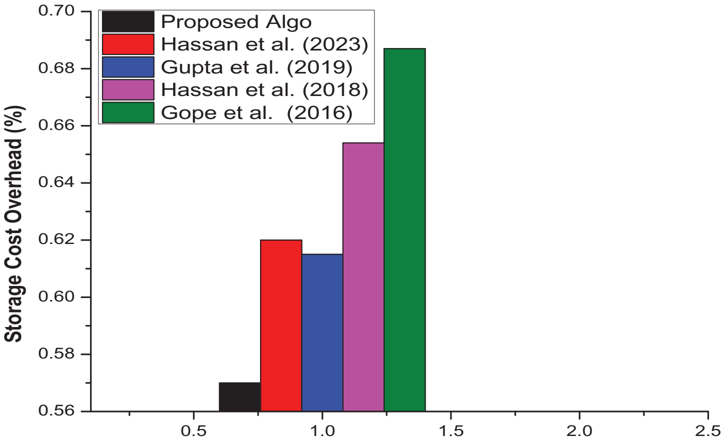

Figure 6: Graphical depiction of the comparative evaluation, particularly in terms of storage cost, of the proposed hybrid and existing state of the art algorithms

4.4 Scalability of the Proposed Approach

The proposed hybrid prediction model doesn't suffer from the scalability issue as it is based on the device and server framework. Therefore, if number of devices and server modules are increased, it will effects the performance as long as the required ratio of server and devices are maintained in the working domain of IoT. Secondly, devices are not required to be member of the respective server module, but this membership is subjected to the RSSI value and slot availability with the concerned server module. Furthermore, if only devices are increased, then it is not necessary that these devices will be deployed in the coverage area of a single server, therefore, the proposed model has the capacity to support additional device even after the network becomes operational.

4.5 Limitations of the Proposed Scheme

Although the proposed authentication model can separate request messages generated by legitimate and adversary modules in IoT, it has certain vulnerabilities.

1. Denial of Service (DoS) is a possible limitation if the adversary module can separate ordinary devices from the server modules in IoT.
2. The proposed authentication model doesn't support the mobility of ordinary devices, which are required in certain application domains, such as smart hospitals, where a patient with wearable devices is moved from the coverage area of one server to another.

5 Conclusion

In this paper, a Hidden Markov Chain Model and an advanced encryption Standard-enabled perpetrator device's prediction algorithm were presented to ensure that only trusted modules (both legitimate devices and edge), i.e., pass through the proper authorization process, are granted permission to initiate a secure transmission thread, particularly on an unsecured channel in the IoT. For this purpose, both modules were required to be part of the offline phase, where secret keys and MaskIds are generated and shared. Secondly, every module, whether it is a legitimate device or an edge, must verify the credentials of another party (the receiving module in this case). For this purpose, a cipher text message is generated by the respective module via its secret key and embeds its MaskID. This message can only be deciphered through a valid key, i.e., λ, and it is a verification to the edge module as it contains a registered MaskID. Additionally, both modules use the hidden Markov chain model to separate legitimate and adversary modules. The proposed scheme was proven to be effective against well-known intruder attacks such as masquerading, eavesdropping, and impersonation. Secondly, the proposed hybrid algorithm requires the minimum possible bandwidth, processing time, and onboard storage, which are 30%, 38%, and 29% in terms of computational, communication, and storage overheads, respectively.

The proposed hidden Markov chain-enabled secure communication model could be extended to cover environments where either devices or edges are mobile, especially in the context of IoT. Device authenticity issues become more challenging if allowed to move from the coverage area of the respective server to another. For example, a patient with wearable devices is moved from one ward or hospital to another for a checkup. Similarly, the same occurs it server modules become mobile. Secondly, multiple edges can be incorporated into the proposed setup, along with mobility where authenticity could be become more challenging as compared to the single edge.

Acknowledgement: The researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support (QU-APC-2025).

Funding Statement: This research work is supported by the Deanship of Graduate Studies and Scientific Research at Qassim University via Grant No. (QU-APC-2025).

Author Contributions: The authors confirm contribution to the paper as follows: Study conception and design: Amjad Khan and Rahim Khan; data collection: Amjad Khan, Rahim Khan and Fahad Alturise; analysis and interpretation of results: Amjad Khan, Rahim Khan, Tamim Alkhalifah; draft manuscript preparation: Amjad Khan, Rahim Khan, Tamim Alkhalifah and Fahad Alturise. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: This article does not involve data availability.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Al-Rasheed RA, Khan T, Alsaed M, Kundi M, Saad HM, Sarker MR. Privacy-preserving information fusion technique for device to server-enabled communication in the Internet of Things: a hybrid approach. Comput, Mater Continua. 2024;80. doi:10.32604/cmc.2024.049215.
2. Wang C, Wang D, Duan Y, Tao X. Secure and lightweight user authentication scheme for cloud-assisted Internet of Things. IEEE Trans Inf Forensic Secur. 2023. doi:10.1109/TIFS.2023.3272772.
3. Gong B, Zheng G, Waqas M, Tu S, Chen S. LCDMA: lightweight cross-domain mutual identity authentication scheme for Internet of Things. IEEE Internet Things J. 2023. doi:10.1109/JIOT.2023.3252051.
4. Zhang L, Li B, Fang H, Zhang G, Liu C. An Internet of Things access control scheme based on permissioned blockchain and edge computing. Appl Sci. 2023;13(7):4167. doi:10.3390/app13074167.
5. Wang F, Cui J, Zhang Q, He D, Gu C, Zhong H. Blockchain-based lightweight message authentication for edge-assisted cross-domain industrial Internet of Things. IEEE Trans Dependable Secure Comput. 2023. doi:10.1109/TDSC.2023.3285800.
6. Ali U, Idris MYIB, Frnda J, Ayub MNB, Khan MA, Khan N, et al. Enhanced lightweight and secure certificateless authentication scheme (ELWSCAS) for internet of things environment. Internet of Things. 2023;24:100923. doi:10.1016/j.iot.2023.100923.
7. Amanlou S, Hasan MK, Bakar KAA. Lightweight and secure authentication scheme for IoT network based on publish-subscribe fog computing model. Comput Netw. 2021;199:108465. doi:10.1016/j.comnet.2021.108465.
8. Kumar P, Chouhan L. A privacy and session key based authentication scheme for medical IoT networks. Comput Commun. 2021;166:154–64. doi:10.1016/j.comcom.2020.11.017.
9. Mbarek B, Ge M, Pitner T. An efficient mutual authentication scheme for internet of things. Internet of Things. 2020;9:100160. doi:10.1016/j.iot.2020.100160.
10. Krishnasrija R, Mandal AK, Cortesi A. A lightweight mutual and transitive authentication mechanism for IoT network. Ad Hoc Netw. 2023;138:103003. doi:10.1016/j.adhoc.2022.103003.
11. Jan MA, Zhang W, Akbar A, Song H, Khan R, Chelloug SA. A hybrid mutual authentication approach for artificial intelligence of medical things. IEEE Internet Things J. 2023. doi:10.1109/JIOT.2023.3317292.
12. Santhanalakshmi M, Lakshana M, GM MS. Enhanced AES-256 cipher round algorithm for IoT applications. Sci Temper. 2023;14(1):184–90. doi:10.58414/SCIENTIFICTEMPER.2023.14.1.22.
13. Liu Y, Dong M, Ota K, Liu A. ActiveTrust: secure and trustable routing in wireless sensor networks. IEEE Trans Inform Forensic Secur. 2016;11(9):2013–27. doi:10.1109/TIFS.2016.2570740.
14. Gope P, Hwang T. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Trans Ind Electron. 2016;63(11):7124–32. doi:10.1109/TIE.2016.2585081.
15. Hasan MM, Ariffin NAM, Sani NFM. Efficient mutual authentication using Kerberos for resource constraint smart meter in advanced metering infrastructure. J Intell Syst. 2023;32(1):20210095. doi:10.1515/jisys-2021-0095.

16. Meddeb Makhlouf A, Guizani M. SE-AOMDV: secure and efficient AOMDV routing protocol for vehicular communications. Int J Inform Secur. 2019;18(5):665–76. doi:10.1007/s10207-019-00436-z.
17. Gupta A, Tripathi M, Shaikh TJ, Sharma A. A lightweight anonymous user authentication and key establishment scheme for wearable devices. Comput Netw. 2019;149:29–42. doi:10.1016/j.comnet.2018.11.021.
18. Hasan MR, Zhao Y, Luo Y, Wang G, Winter RM. An effective AODV-based flooding detection and prevention for smart meter network. Procedia Comput Sci. 2018;129:454–60. doi:10.1016/j.procs.2018.03.024.
19. Li X, Ibrahim MH, Kumari S, Sangaiah AK, Gupta V, Choo KKR. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Comput Netw. 2017;129:429–43. doi:10.1016/j.comnet.2017.03.013.
20. Abdelshafy MA, King PJ. AODV and SAODV under attack: performance comparison. In: Ad-Hoc, Mobile, and Wireless Networks: 13th International Conference, ADHOC-NOW 2014; 2014 Jun 22–27; Benidorm, Spain: Springer; p. 318–31.
21. Gope P, Das AK, Kumar N, Cheng Y. Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. IEEE Trans Ind Inform. 2019;15(9):4957–68. doi:10.1109/TII.2019.2895030.