Wireless Networks (2023) 29:1333–1354
https://doi.org/10.1007/s11276-022-03197-1

ORIGINAL PAPER

Secure user authentication and key agreement scheme for IoT device access control based smart home communications

Sirisha Uppuluri[1] · G. Lakshmeeswari[1]

Accepted: 18 November 2022 / Published online: 3 December 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

The upcoming paradigm in Internet of Things (IoT) based applications is to afford effective interactional communication strategies between the devices in the smart home system. With the rapid growth of IoT services, the incorporation of security measures becomes a vital concern. The general issue faced in the security of the intercommunication between the devices and the users is improper authentication between them. Also, the access control of devices must be ensured with reliable features for establishing secure communication between the users and devices. Hence, we propose a protocol called Modified Honey Encryption using Inverse Sampling-Conditional Probability Model Transform (MHE-IS-CPMT) with Elliptic Curve Cryptography (ECC) to authenticate and perform the key agreement. Here, we employ the following steps: (1) Initialization, (2) Registration, (3) Login and data access Request, (4) Authentication and Session key agreement, and (5) Key update. At the commencement of the session, the users (u), Mobile Users (MU), and the other devices participating in the smart home system are initialized to the Home network head (H). Then, for the registration process, the user and the devices register them into H via the smart gateway (SG) by providing their own identities. The user details and the data about the devices are secured using the MHE-IS-CPMT with the ECC method. Next, during the login process, the registered users connect to the smart home system and send a request to SG to gain access to the devices. After verification, the user is authenticated and the system enables them to acquire the device access control by providing them with the private key of the device. In addition, the proposed system facilitates the secure key change procedure for the legitimate user to update their key whenever required. Hence, the performance of the model is secured against different types of attacks and also obtains more security features than existing methods.

Keywords Internet of things (IoT) · Authentication · Key agreement · Smart home · Security · Device access control · Attacks

1 Introduction

In today's world, there has been a huge development in superior integrated services for smart home automation systems. With the rapid integration of the Internet of Things (IoT), the internet-enabled smart services are connected with the operation of controlled software and hardware components that communicate with each smart device to facilitate a high-tech lifestyle [1]. Due to the wide availability of the internet, intelligent devices are tremendously increased and reach 50 to 100 billion by the year 2020 [2]. In the IoT ecosystem, the physical devices include actuators and sensor networks, and other software settings are used in different applications such as medical, industrial, civic, etc., [3]. The embedded devices are integrated with IoT to connect with a large number of devices and provide users trusted gain in the smart environment [4]. Mostly, the consumers focused on "smart home" devices like cameras, video door locks, light bulbs, motion sensors, smoke detectors, thermostats, etc. [5] These devices are responsible for safety–critical functionality built-in web servers that allow accessing its information online for daily requirements. So, the application of device-to-device and app-to-device or user-to-device access control information is sensitive for the third-party servers [6, 7]. However,

✉ Sirisha Uppuluri
phd.sirishauppuluri01@gmail.com

[1] GITAM University, Visakhapatnam, Andhra Pradesh 530045, India

accessing the services of IoT based smart home device assessment methods needs security due to its heterogeneous nature at each operation.

Likewise, the constrained devices are lying to renowned attacks such as Denial of Service (DoS) attacks, replay attacks, and cryptography attacks [8, 9]. These security attacks are solved with cryptographic solutions to achieve the goals of data integrity, confidentiality, and availability [10]. Recently, access control and device authentication mechanism are some of the main security problems in smart home-based IoT environments. In the access control system, the capability-based access control model ensures end-to-end security by Internet Protocol Security (IPsec), and accessing devices in the group are supported using a single token. The accessed groups are determined using Unique Local Address (ULA) [11]. Also, the type of different access levels is provided to different agents using the user-managed access model [12]. But in large scale networks, the distributed network uses an attribute-based cryptography method in which the attributes are assigned with user permissions and changed easily with the absence of access structure [13, 14].

In the authentication mechanism, the three-level Kerberos secure mechanism uses Advanced Encryption Standard (AES) and SHA-1 hash algorithm for constrained smart home-based IoT devices [15]. The verified controller node identity minimizes handshake overhead and secures man-in-the-middle attack using Threshold Cryptography based Group Authentication (TCGA) scheme [16]. For secure communication, the shared key security mechanism is used with the digital certificate supported by the certificate authority to make the authentication more robust between the devices [17]. Moreover, the mobile IoT devices run on Wi-Fi gateway node and network for users to device configuration that initiates authentication process from the gateway to IoT device. This process is integrated with ECC for a key generation [18–20]. The above-presented methods of authentication and access control mechanism face problems in data transmission to the server. Also, an attacker can invade the user's private information connected with smart devices by eavesdropping and DoS attack. The existing approaches suffer from a lack of security between the users and smart devices. Therefore, a secure key agreement based encryption mechanism should be designed that needs to supply further attention in IoT connected devices and provide security between users and devices at low cost.

1.1 Motivation

The current research on IoT is an interesting field of concern in smart home automation systems in which authentication and access control mechanisms are a major challenge to deal with several applications such as the smart devices that are used can include smart lights, air control, washing machine, smoke detector, door sensor, surveillance cameras, smart media, central AC etc. [21]. For example, IoT technology can be used to identify devices, users, or natural people's access control such as attempted logins, service requests, access durations, and location, based on both IP and Bluetooth at smart homes, reducing strain on resources while monitoring people continuously and enabling them to stay at home longer, connected over the internet. In order to access services and manage IoT devices, users communicate with IoT networks through their end devices. The smart devices only transmit signals when the home owner is not at home. Limiting access to authorized entities (data owner, mobile user, IoT devices) is critical for ensuring data confidentiality against various types of attacks. Attackers can gain access to a system and steal information when user authentication is not secure [22].

Several existing methods, such as lightweight encryption [23], cryptography algorithms [24], and lightweight mutual authentication [25], perform data assessment on IoT devices, raising many security threats as well as efficiency issues in the system. The existing techniques concern the home server trust factor, which has complete access control to secure the user's private information on smart home platforms. But it cannot be leveraged on a secure access service. Moreover, the requested services gather the inside and outside information and encrypt the data before sending it to the server, which leads to security problems when using multiple requesting services to the server. Problems encountered in home communication between the device and user accessing data have been addressed in many existing methods. But an attacker can access the data in between the device and user communication. Motivated by these facts and existing studies, there is a need to overcome the security issues using key agreement and authentication algorithms that address the enforcement of IoT devices and access services of user-to-device applications.

1.2 The major contributions are summarized as follows

- For secure authentication and key agreement in the smart home system, MHE-IS-CPMT with ECC is proposed in access control of IoT devices present in the smart home. Here, the user and device data are secured by the MHE with the keys generated using the ECC scheme.
- The security of the protocol is evaluated for different commonly occurring attacks in the IoT environment and hence the proposed protocol is resilient to different types of attacks. The proposed protocol confuses the

adversaries in the system by sending them plausible data instead of the original sensitive smart home data.

- Moreover MHE-IS-CPMT with ECC protocol is simulated using the Python tool and then its performance efficiency is compared with other recent approaches.

The paper structure is organized as listed as follows. Section 2 provides a brief description of the existing works. Next, Sect. 3 provides the preliminaries of the system used in smart home security. A detailed description of the system model is provided in Sect. 4. In Sect. 5, the security of the proposed MHE-IS-CPMT is analyzed in detail. Section 6 conveys the comparative analysis for the performance efficiency of the proposed system. The limitations of the proposed work is presented in Sect. 7. The entire working process is concluded in Sect. 8.

2 Related works

Many research scholars have done a different aspect of authentication and key agreement methods and its issues on recent smart home systems are discussed below.

Chifor et al. [26], presented a lightweight authorization scheme for secure communication between the users and smart devices in IoT platforms. In this approach, a security stack scenario is used to interact between the web services and embedded devices for establishing the infrastructure through the IoT connected devices. The deployed smart home infrastructure has heterogeneous IoT devices where connected devices are accessed by a digital identity and communicate the response to another device service for authorization. This IoT based security architecture is considered a trusted module. After authorization, the user to device-centric data is secured by a Fast IDentity Online (FIDO) protocol. Thus the approach preserves user anonymity among the information linked by the user and the outcome shows a low impact on smart applications.

Shen et al. [27], introduced a key agreement and secure transport strategy for Home Area Networks (HAN). The smart home system faces security issues such as data integrity for data upload and smart gateway in data monitoring. For this purpose, the approach uses a secure data uploading scheme to verify whether any malicious gateway monitors the data or not. In this, the uploaded data is accessed by a home gateway based session key from the smart home environment. Hence the approach prevents malicious gateways while uploading the data. Furthermore, the security analysis proves that the approach ensures efficient security for uploading data. Similarly, verification of data integrity is also required for secure data uploading.

Anthi et al. [28], mentioned an IoT infrastructure system that incorporates a supervised approach called a 3-layer system for intrusion detection to determine security flaws on smart home-based IoT platforms. This system involves three entities: the first entity describes that the normal behavior of the IoT device profile and type is classified, and each device is connected to the smart home network-based IoT devices. Secondly, the network system determines that the transmitted packets are malicious on the network. Lastly, the deployed network classifies the type of attack in the system. Thus, the performance is evaluated with the machine learning approach for the network activity and automated function from real testbed parameters. This concludes that the IDS detects the attack deployed on the networks. However, the network does not support automatic detection.

Yan et al. [29], introduced a function-based access control authentication scheme between the home gateways and smart devices in IoT (FBAC-IoT). Each smart device has a unique ID with a number of functions for fine-grained access control in the home environment. In this, the varying number of function generates different data agrees with the hub. This scheme uses the Identity Based Encryption (IBE) method to access encrypted data before uploading it to the server, which ensures data privacy. Using this approach, only the authorized data is accessed and obtains the ciphertext to decrypt the function, else it will terminate the request. Since the FBAC-IoT scheme computational cost is constantly maintained for each operation and security proofs analyzed that the FBAC-IoT approach prevents privilege access among the devices.

Alshahrani et al. [30], presented a lightweight mutual authentication for edge devices with secure resource constraints in the IoT environment. In this case, the key exchange protocol and authentication method depend on the cumulative keyed-hash function and temporary identity. The authenticated nodes with the session are established by dynamic identities. Moreover, a virtual domain segregation setup ensures the security policy for the transmission and reception capability of nodes commands for inside attacks. The cumulative keyed-hash function is responsible for verifying the identity of the sender by a challenging command. In addition, this approach improves identity guarantee by using the concept of fog computing. Hence the performance is estimated using AVISPA toolkit and informal security analysis is proofed using BAN logic.

Punithavathi et al. [31], presented a secure lightweight authentication scheme based on cancelable biometric system (CBS) in the cloud environment. Initially, the biometric image processing step involves, Region of Interest (ROI), thinning, Binarisation, and histogram localization. Then the general process of the feature extraction step is obtained. Lastly, the matched templates are recovered and retrieved in the Cancelable Template Database (CTD). Then the new transformation of the authenticated key is generated by a new cancelable template. The evaluation considers real-world settings to authenticate the device data with less overhead and high accuracy. Furthermore, this approach is supported in smart IoT surroundings.

Naik et al. [32], presented an IoT based smart house management system that combines microcontrollers, actuators, smartphones, and web services. This method is cost effective and energy efficient, but time consumption is more. Furthermore, Gochhayat et al. [33] suggested a distributed key management solution for IoT security. This technique effectively secures IoT devices by transferring the majority of resource-intensive cryptographic operations to a local entity. This method has less communication overhead and generation time. However, storage cost is high.

Mansoor et al. [34], introduced an improved lightweight authentication protocol to secure Radio Frequency Identification (RFID) systems against known attacks in IoT networks. Each RFID system consists of three entities (database server, reader device, and tags) using Burrows Abadi-Needham (BAN) logic to analyze the security features. From the simulation of informal and formal security analysis, this protocol is suitable for practical IoT applications. However, this protocol is time consuming during transaction.

Shahid et al. [35], presented a Proficient Security over Distributed Storage (PSDS) method to solve the data security issues during data transmission on multi cloud. For this purpose, the cloud database splits the data into two sections: sensitive and normal. The normal data formation was encrypted and uploaded by a single cloud whereas the sensitive data is also encrypted and distributed via multicloud. Hence the PSDS method stores the data securely against multiple attacks. But the PSDS method cannot promote to validate the key agreement by trusted authority between user and cloud service.

Samuel et al. [36], presented a privacy infrastructure based on federated learning and blockchain technology to manage and reduce the risk of healthcare centers during transmission in Internet of Medical Things (IoMT). This privacy model was used to improve public communication and resolve large data silos when the data owner privacy was preserved, particularly for COVID-19 patients. Overall, the privacy infrastructure model was resistant to security-based attacks, but it cannot guarantee that the patient has been verified by the data owner.

The summary of several approaches involved in IoT based smart home device applications is shown in the Table 1.

The above-mentioned schemes discuss the advantages and drawbacks which is most viable to smart home-based IoT applications. On analyzing the presented mechanism, it is prone to several disadvantages such as it is less effective in accessing the device control, less privacy due to repeated request services, and less secure due to several attacks. Also, the system raises issues in communication that concerns delay, throughput, cost, and complexity. Therefore, there is an efficient secure authentication mechanism is required in IoT based smart home environment to address all issues determined in the existing systems.

3 Preliminaries

In this section, the details regarding the basic functionalities of the secure authentication and key agreement schemes is presented.

3.1 Smart home

It is a home that is fully equipped with automated device control applications that can be managed or supervised from a remote location using a computer or smartphone device. The attributes of the home such as the temperature sensors, lightings, appliances, entertainment systems, alarm systems, etc. are connected through the internet. For enabling the control over these devices, the system use web interface, applications in mobile phone, desktop computers, etc. However, these automation face issues due to the inadequacy in the standards of security measures provided to the system. The current state of smart home automation requires a considerable capacity to exchange data between the members of the family or only on the trusted individuals.

3.2 Adversarial model

The model assumes that an adversary tries to attack the smart home system and breaches the system to launch attacks. The assumptions of the adversary model are described as follows.

1. Any internal or external attacks on the system may compromise an adversary (β). This type of attack justifies that the attacker can steal the traffic data access center files (content of request files) between the connection of the home network head and the smart gateway sent by the user.
2. An attacker can acquire access to data over the communication channel. This type of attack can destroy the access data of the smart device and extract the sensitive information of user entities stored in the home network head.
3. The identities of the user, device, SG, and H are known to the attacker. This type of attack can falsify each entity's network access data over the network.
4. Adversaries do not have the ability to change, replay, or shift any user data content. This attack is sufficiently

Table 1 Summary of existing approaches in IoT based smart home applications

Author/year	Technique used	Goal	Advantage	Limitations
Chifor et al. [26], 2018	Lightweight authorization scheme	To preserve user anonymity among the information linked by the user and smart devices in IoT platforms	Device to device access data is secured	Low impact on smart applications
Shen et al. [27], 2018	Key agreement and secure transport strategy	To upload the access data by a home gateway based session key for HAN	Ensures efficient security while uploading data	Less probable on data integrity
Anthi et al. [28], 2019	3-layer IDS method	To determine security flaws on smart home based IoT platforms	This scheme detects attacks on the networks	The networks does not support automatic detection
Yan et al. [29], 2019	FBAC-IoT	To access control in fine-grained resources from home environment	This scheme protects smart applications from unauthorized accessing functions	Only the device privilege is secured
Alshahrani et al. [30], 2019	Lightweight mutual authentication scheme	To secure edge devices using cumulative keyed-hash function and temporary identity	Less probable on inside attacks	High computational cost
Punithavathi et al. [31], 2019	Lightweight authentication scheme based on CBS	To secure device authentication using biometric process in cloud environment	Low overhead High accuracy	High execution time
Naik et al. [32], 2018	Smart house management system	To manage the system devices	Cost effective and energy efficient	High computation time
Gochhayat et al. [33], 2020	Distributed key management solution	To effectively secures IoT devices by transferring the majority of resource-intensive cryptographic operations	Less communication overhead and generation time	High storage cost
Mansoor et al. [34], 2019	Improved lightweight authentication protocol	To secure RFID systems against known attacks in IoT networks	Suitable for practical IoT applications	High running time during transaction
Shahid et al. [35], 2020	PSDS	To solve the data security issues during data transmission on multi cloud	Stores the data securely against multiple attacks	Cannot promote to validate the key agreement
Samuel et al. [36], 2022	Federated learning and blockchain technology	To manage and reduce the risk of healthcare centers during transmission in IoMT	Resists security based attacks	Cannot guarantee that the patient has been verified by the data owner

absent in strong login passwords due to hacker login between the user terminals.

5. An adversary can gain access through the links (linkability attack) between the communication of a user and the home server. In this, unauthenticated access allows threat actors to gain access to an IoT device, which makes it easy to exploit device data.

3.3 Honey encryption (HE)

HE is a security tool to secure the data between the user and devices present in the smart home system [37]. This encryption process divides the user data into a set of sequences called the message set and stores them in the message space. Before encryption of the user data, the required message space must be predicted. Then, the message sequence is arranged in some order and the probability of occurrence of the message in the space is predicted. Next, an encoder is used to map the sequences into the seed space. Also, it is ensured that the number of mapped sequences of user data is equal to the number of spaces occupied by them in the space. The seed space must be large enough such that the message is mapped to a minimum of one seed. The major benefits of using the HE process is used to protect data stored on password manager services that will confuse the intruders or adversaries by sending plausible data similar to the original data for secure transmission.

3.4 Elliptic curve cryptography (ECC)

The most common method for key generation is the Elliptic Curve Cryptography (ECC) [38] that is used widely due to

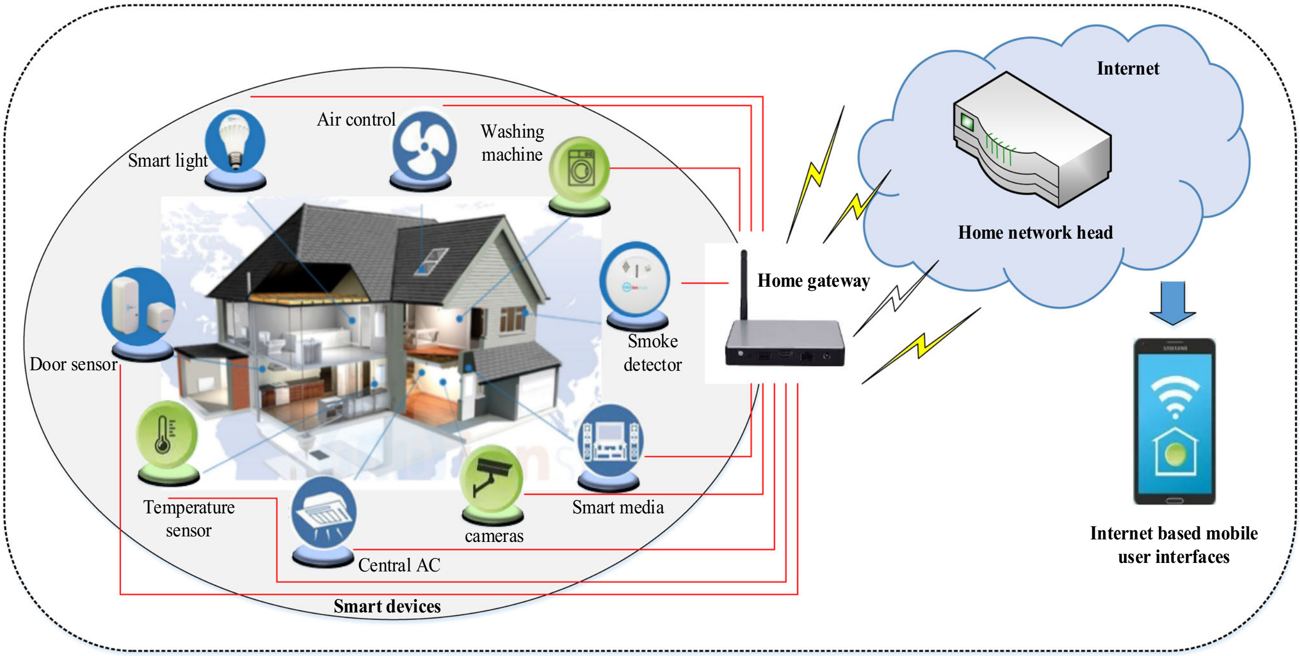


Fig. 1 Smart home system model

its easier working process. ECC generates a public–private key pair for the encryption. The public key is transferred to all the users and servers of the system whereas the private key is known only to the user. The key exchange mechanism is secured using the Diffie Helman Key exchange process. For the generation of the private key, the secret parameters are computed in the system from the ASCII encoding of the user id and password. This key generation assists in secure data transmission in the smart system. The seed generated by the HE process is XORed with the keys to generate a ciphertext for storing the valuable user data.

4 Proposed MHE-IS-CPMT framework

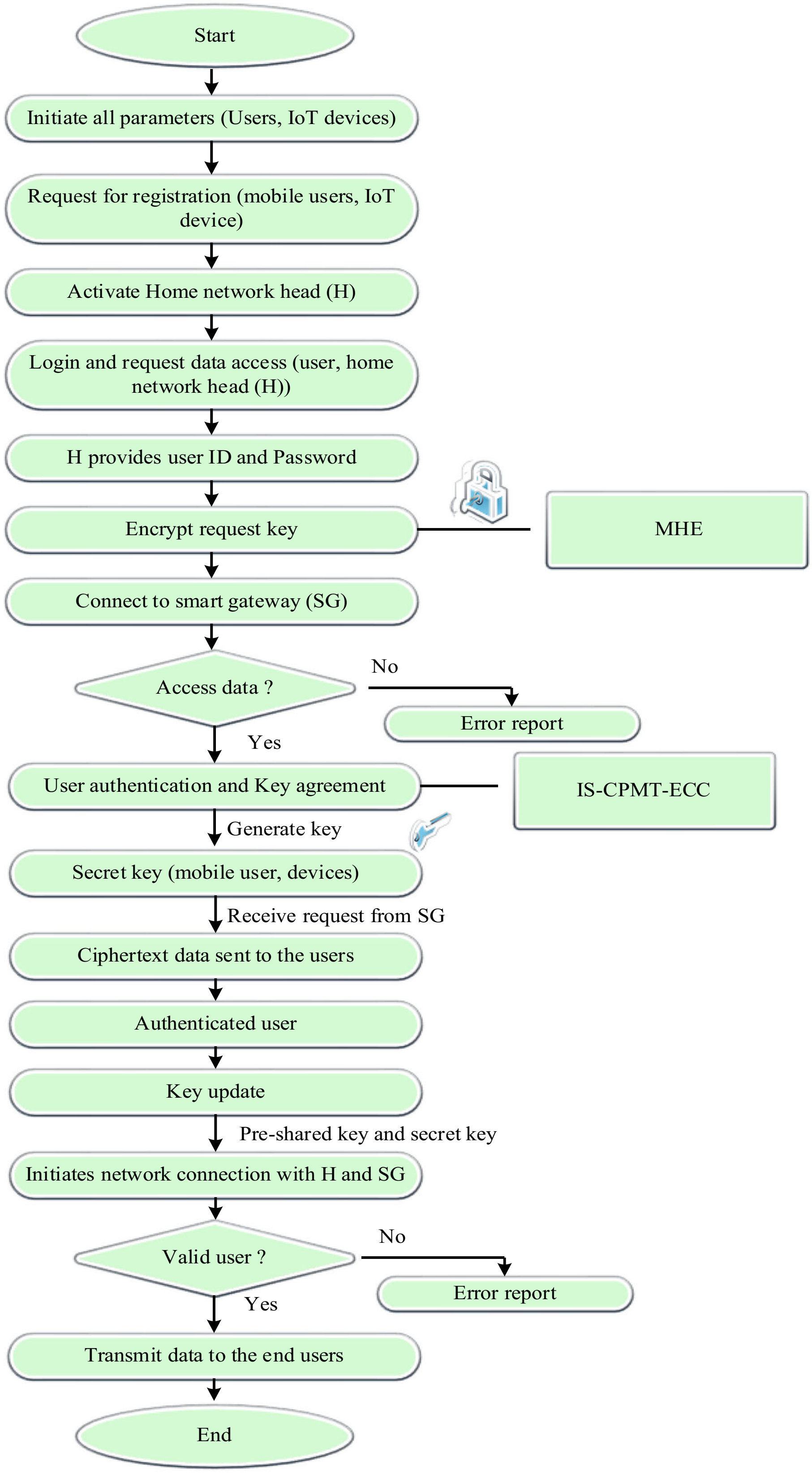
In the proposed methodology, we present a session key agreement and authentication scheme based upon Modified Honey Encryption using Inverse Sampling-Conditional Probability Model Transform (MHE-IS-CPMT) and Elliptic Curve Cryptography (ECC) that secures access data for a large number of IoT devices, which is more vulnerable to attacks from different sources. This algorithm helps in protecting smart home applications from attackers by generating plausible data. This plausible data generation will confuse the attackers as the provided data is similar to the real one. First, the device and user installation steps are performed to initiate all parameters. Then, the registration step is performed between the mobile user and IoT devices for registration request submission and device activation in the home network head. Next, the login and data access request step is performed between the home network head and user to verify the request data through the home gateway. Then the authentication and session key agreement steps are secured by concatenating the seed obtained from the honey encryption and the key is generated by ECC and only the ciphertext is sent to the users. The data accessed by the device is provided only to the authenticated user at the time of the request. Lastly, the key update step is performed based on the authenticated user with the valid secret key of each parameter for the mobile user and devices. Thus, the proposed security architecture is a reliable communication network and the accessed data allows only registered users to participate in the data transmission and also mitigate attacks. The smart home system model is shown in Fig. 1, and the flowchart of the proposed model is shown in Fig. 2.

4.1 System model

There are five different entities such as Users (u), Smart gateway (SG), Mobile user (MU), IoT devices (N), and Home network head (H). The process flow of the proposed system is categorized into five phases.

1. *Installation Phase of IoT Devices and Users:* This is the initial phase in the device access control of IoT. Here, *u*, *MU*, and *N* are initialized to *H*.
2. *Registration Phase:* In this, each user sends a request for registration and activate the device function.

Fig. 2 Flowchart of proposed model


Start
Initiate all parameters (Users, IoT devices)
Request for registration (mobile users, IoT device)
Activate Home network head (H)
Login and request data access (user, home network head (H))
H provides user ID and Password
Encrypt request key
MHE
Connect to smart gateway (SG)
Access data ?
No
Error report
Yes
User authentication and Key agreement
IS-CPMT-ECC
Generate key
Secret key (mobile user, devices)
Receive request from SG
Ciphertext data sent to the users
Authenticated user
Key update
Pre-shared key and secret key
Initiates network connection with H and SG
Valid user ?
No
Error report
Yes
Transmit data to the end users
End

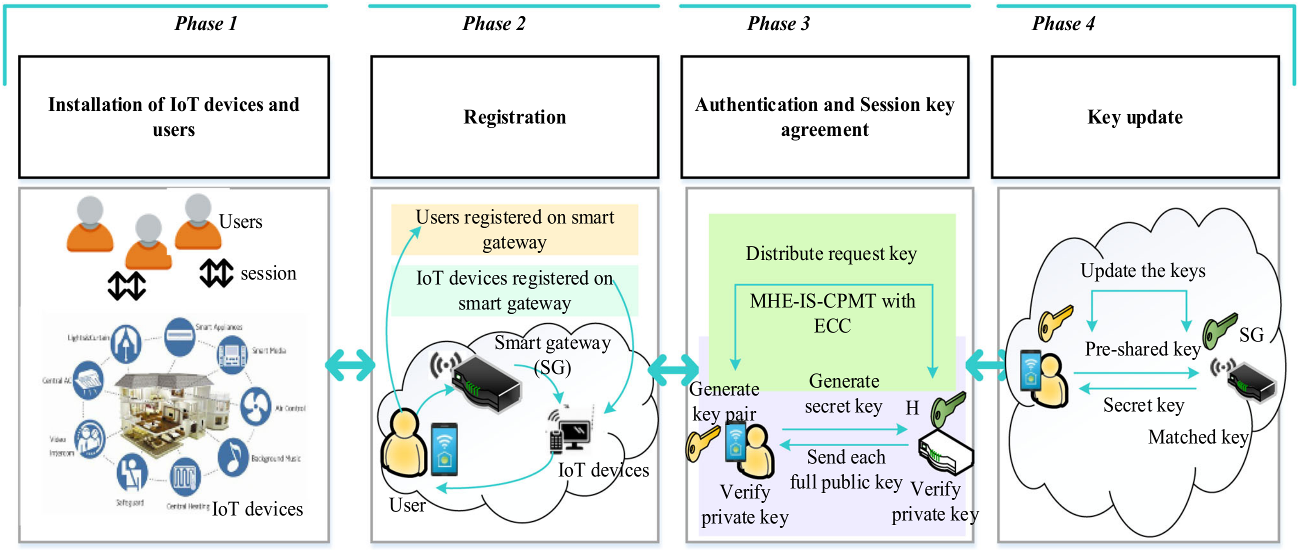


Fig. 3 Proposed graphical model

3. *Login and Data Access Request Phase:* Here, legitimate users are allowed to login and request access control of the different IoT devices.
4. *Authentication and Session Key Agreement Phase:* The system allows only legitimate users to access the devices through an authentication mechanism using a key-based agreement scheme.
5. *Key Updating Phase:* Users can change and update the keys provided to them by selecting their own secret parameters. The overlay of the proposed security architecture graphical model for IoT device-based home communication is shown in Fig. 3.

The symbols used and its description is provided in Table 2.

A. Installation phase of IoT devices and users

The basic requirement of providing smart facilities in the home involves the installation of smart devices. The installations follow the setup procedure for the devices in the smart home. This is the process of making the smart devices prepared for activation and execution of routine activities in the smart home environment. Consider n be the number of devices in the smart home system.

a. *User Installation*

Step 1: The users $u_1, u_2, ..u_x$ or the mobile users $MU_1, MU_2, ..MU_x$ are initialized into the smart home system with their name and the membership in the family. Then, H issues u_id and password of the user pw_user to every initialized users $u_1, u_2, ..u_x$.

Step 2: A key for encrypting the requests made by the user req_key is maintained by the network. These pre-shared parameters are secretly stored into the

Table 2 Symbols used and their notations

Symbols	Description
u_x/MU_x	Users/mobile users
H	Home network head
SG	Smart gateway
C	Certificate
UC	User credentials
n	Number of devices
u_id	User identity
ud_x	User details
H_{u_x}	Sequence user details
$CP^{(d)}(H_{u_x})$	Conditional probability of sequence user details
pw_user	User password
u_req	User request key
χ	Device activation function
dev_id_i	Device identity
ran_keyw	Random keyword
$pw_{dev\_id_i}$	Device password
pub_key,pri_key	Private key and Public key
req_key, $Sess\_key$	Request key and session key
t_{st}	Timestamp
e_{u_i}, r_{u_i},w_i,o_i	Secret parameters
$L_{\max}$	String y of length
$(y_i)_i$	String for y-bits
ψ_i	Random fields
$k,,j$	Random parameter
y	Storage overhead
S	Message space
P	Probabilistic random generator
k	Random number

internal memory by the producers *P* of the device to help in future communication. After initialization, *H* issues a certificate (C) to (n) devices in the system.

b. *Device Installation*

Step 1: Initially, the installation step is carried out in the *H* that requires the inherent of device id (dev_id_i) with a random keyword (ran_keyw) and a password ($pw_{dev\_id_i}$), this can be expressed as,

$$P \to dev_i\{\, dev\_id_i, ran\_keyw, pw_{dev\_id_i}\} \tag{1}$$

Step 2: Here, $pw_{dev\_id_i}$ is considered to be secret such that *P* computed as,

$$pw_{dev\_id_i} == hash\,(dev\_id_i||\,k) \oplus ran\_keyw \tag{2}$$

where *k* is considered as a random number generated using the probabilistic random generator.

Step 3: Consider the parameters for future evaluations of Elliptic curve *EC* under random fields (ψ_i). Then choose *j* as a random generator in a group *H* with order *l*.

Step 4: Choose a private key such that $key\ \varepsilon H_l^*$ and then predict the public key,$pub\_key = pk * j$.

their credentials. Two types of registrations are carried out in the system, such as user registration and device registration. For secure storage and utility of the smart service, modified honey encryption algorithm is employed. Here, we propose the IS-CPMT process in honey encryption for user data encryption, which is incorporated with the keys generated using the ECC. It employs a strong fixed field for the generation of cryptography and proceeds with the signature and verification mechanisms of the user.

a. User registration

Users of the smart home is confined to the members of the family since leakage of the smart home data is a serious issue affecting the privacy of the user. SG has the ability to store some information about user details because of convergence to the randomized strategy point of the internal network. It also enables users to securely aggregate, process, and filter data based on the connection of Wi-Fi and ZigBee. Then, it transfers the user details to H for encryption using HE. In between the encryption process, the user login terminals frame the public key using another secret parameter incorporated with the generated private key using the Diffie–Helman ephemeral key exchange mechanism. Therefore, only the initialized users are allowed to actively participate in the registration process.

***Algorithm.1.* Installation phase**

```
Input : $dev\_id_i$, $ran\_keyw$, $pw_{dev\_id_i}$,
Output : $u\_id$, $pw\_user$ and C

Procedure D_ UserRegister ($u\_id$, $pw\_user$), DeviceRegister ($dev\_id_i$, $pw_{dev\_id_i}$)
    Install H ($dev_i\{dev\_id_i, ran\_keyw, pw_{dev\_id_i}\}$)
    Compute $pw_{dev\_id_i} = hash(dev\_id_i \| k) \oplus ran\_keyw$
    Choose private key ($key\ \varepsilon H_l^*$) and predict public key ($pub\_key = pk * j$)
    Initialize $MU_x(u\_id, pw\_user)$
    Encrypt user ($req\_key$)
    Store pre-share parameters and issue H (C $\to N$)
end procedure
```

The process flow of the proposed scheme is illustrated in Fig. 4.

B. Registration phase

Registration involves gathering the details about the entities and further enrolling them in the system to achieve the activation of the device and acquire services from them. In this phase, a user request (u_req) is send for registration and device activation (χ) is achieved. Here, each entity in the system *(u, SG, N, and MU)* are registered into *SG* using

Step 1: For *'x'* number of users ($u_1, u_2, ..u_x$), compute the user details such as identity of the user (u_id), password of the user (pw_user) which is computed with the randomized strategy ($rand * pw$) for storage into *SG.*

Step 2: SG transfers the user details ($ud_1, ud_2, ..ud_x$) into *H* for encryption. ECC is applied to develop a public and

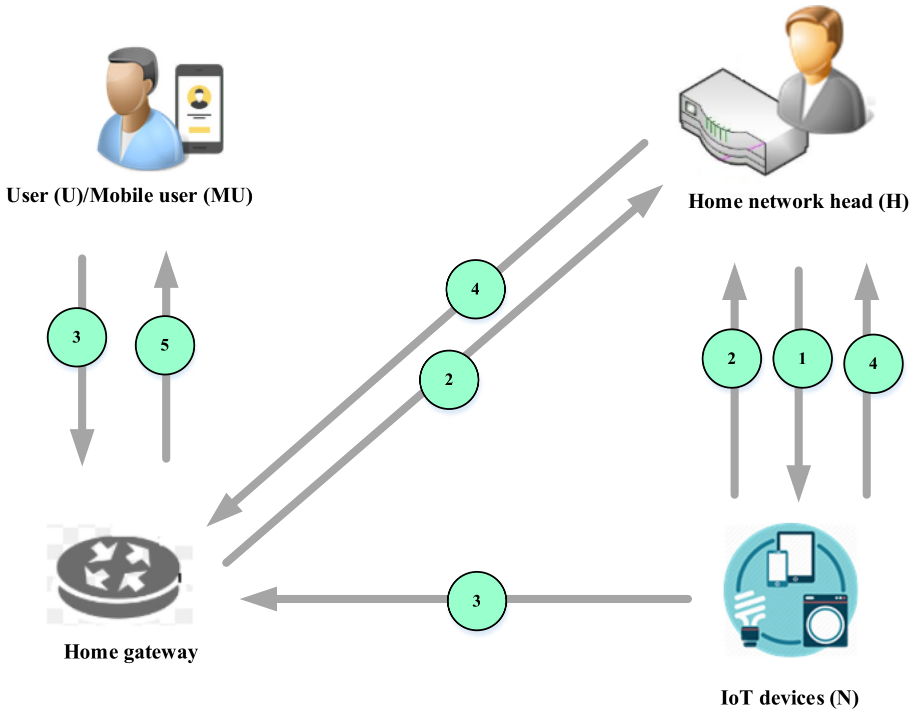


Fig. 4 Process flow of proposed scheme

private key pair. Frame suitable private key (pri_key) for the user using the parameter (e_{u_i}) framed corresponding to the ASCII encoding of the user password (pw_user), which is expressed as,

$$pri\_key = e_{u_i}||pw\_user \tag{3}$$

Step 3: Then, frame the public key (Pub_key) using another secret parameter (r_{u_i}) incorporated with the generated private key expressed as,

$$pub\_key = r_{u_i}||pri\_key \tag{4}$$

where the pri_key is distributed only to the registered u_i and also kept secured in H via SG using the Diffie–Helman Ephemeral key exchange mechanism and u_i provides the signature for the key using the secret parameter (e_{u_i}).

Step 4: Apply modified honey encryption algorithm that employs IS-CPMT for encryption and secure the storage of user details. Consider the storage overhead parameter to be y. Determine the possible number of message space (S) to store $ud_1, ud_2, ..ud_x$ in H. Sample user details into several units $(H_{u_1}, H_{u_2}, H_{u_3}, ..H_{u_x})$ and acquire the possible generating sequences $(H_{u_1}, H_{u_2}, H_{u_3}, ..H_{u_x})^{-1}$.

Step 5: Find the conditional probability $CP^{(d)}(H_{u_x})$ for each sequenced unit $H_{u_x}^{-1}$ and perform discretization of the sequence $CP(H_{u_i}|H_{u_1}, H_{u_2}, ..H_{u_X})$. Unlike the other methods conditional probability needs a condition for encoding the user data.

The condition is defined for each sequence before encoding them. Here, the transformation model is suggested for the conditional probability model that involves the shifted factor to the user data. Then, select any sequence at random (seq_rand) in $H_{u_x}^{-1}$ with $CP^{(d)}\left(H_{u_x}^{-1}|u_x\right)$ is computed as,

$$CP^{(d)}\left(H_{u_x}^{-1}|u_x\right) = \frac{CP^{(d)}(H_{u_x}^{-1}) \oplus (H_{u_x} \mapsto H_{u_x} + a)}{\sum_{i\in 1..n} CP^{(d)}(H_{u_x}^{-1}) \oplus (H'_{u_x} \mapsto H'_{u_x} + a)} \tag{5}$$

where $CP^{(d)}\left(H_{u_x}^{-1}|u_x\right)$ involves shifting the stored message and enables padding of zeros between them. Here, $H_{u_x} \mapsto H_{u_x} + a$ is the shift in data bits of the user.

Step 6: Sort the units based upon suitable order and map the data into suitable seed space. Then, choose a sequence with more probability and encode each sequence with IS-CPMT. Encode each sequence by the IS-CPMT $(|H_{u_1}, H_{u_2}....H_{u_x})$ to y-bit string (str_u_x).

Step 7: Concatenate the strings $(y_i)_i$ then pad the string with string y of length $(L_{\max})$ with random bits and output G seed.

Step 8: Choose an arbitrary number (D_i) in the field ψ_i and multiply it with G. Then, XOR the seed with pri_key and pub_key of the user and output the cipher to u such that $\{cipher \leftarrow (G \circ pub\_key||pri\_key)\}$. The process of IS-CPMT is shown in Fig. 5.

b. Device registration

Step 1: Initialized devices sends a request (req_reg) to SG into the system. For *'n'* devices $\{dev\_id_1, dev\_$

$id_2, ...dev\_id_n\}$, SG acquires $(dev\_IP,\ U\_code,\ \Pr o\ \_code)$ from the device. Also, the certificate C is uploaded into *SG.* The collected details are transferred to H and it verifies the C sent by the device to match with the C issued by H during initialization.

Step 2: If C is matched, for every device (dev_i) the public key and private key generation is performed using ECC and sends the accept message $(accept\_msg)$ along with *Pub_key* to the device and enables them to get registered into *H.*

Step 3: The details about the device is secured by employing the same procedure followed for encrypting the user details using the modified honey encryption.

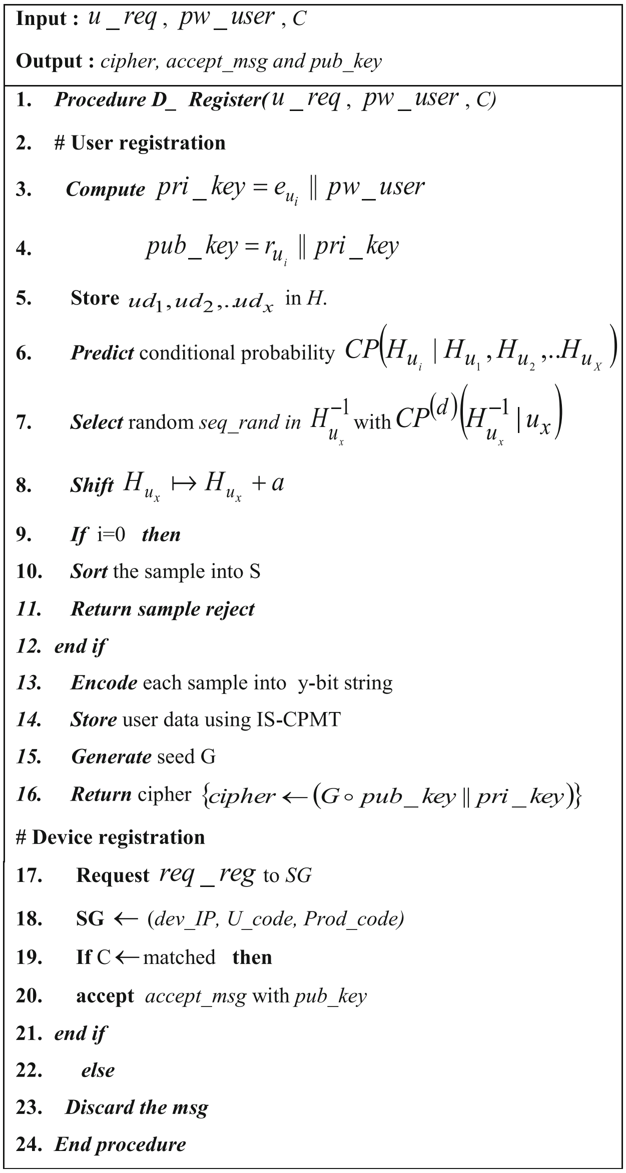
C. Login and data access request phase

In this phase, the users of the IoT system $(u_1, u_2, ..u_x)$ or any registered mobile user login to get access of any devices $\{dev\_id_1, dev\_id_2, ...dev\_id_n\}$ present in *H.* Any user u_i inputs the *cipher* and *pub_key* along with a *access_req* message to *SG.*

Step 1: The login is initiated after verification of the keys and cipher of the user. Only the registered user can participate and access data from the IoT devices. For this, the user credentials (UC) are given to *H.*

Step 2: *H* verifies the user data by deciphering the user input using the *pub_key.* Here, the inverse of XOR is

***Algorithm.2.* Registration phase**



```
Input : $u\_req$, $pw\_user$, $C$
Output : cipher, accept_msg and pub_key
Procedure D_ Register($u\_req$, $pw\_user$, $C$)
# User registration
  Compute $pri\_key = e_{u_i} \parallel pw\_user$
          $pub\_key = r_{u_i} \parallel pri\_key$
  Store $ud_1, ud_2, .. ud_x$ in $H$.
  Predict conditional probability $CP(H_{u_i} \mid H_{u_1}, H_{u_2}, .. H_{u_x})$
  Select random seq_rand in $H_{u_x}^{-1}$ with $CP^{(d)}(H_{u_x}^{-1} \mid u_x)$
  Shift $H_{u_x} \mapsto H_{u_x} + a$
  If i=0 then
  Sort the sample into S
  Return sample reject
end if
  Encode each sample into y-bit string
  Store user data using IS-CPMT
  Generate seed G
  Return cipher $\{cipher \leftarrow (G \circ pub\_key \parallel pri\_key)\}$
# Device registration
   Request $req\_reg$ to $SG$
   SG ← (dev_IP, U_code, Prod_code)
   If C ← matched then
   accept accept_msg with pub_key
end if
   else
  Discard the msg
End procedure
```

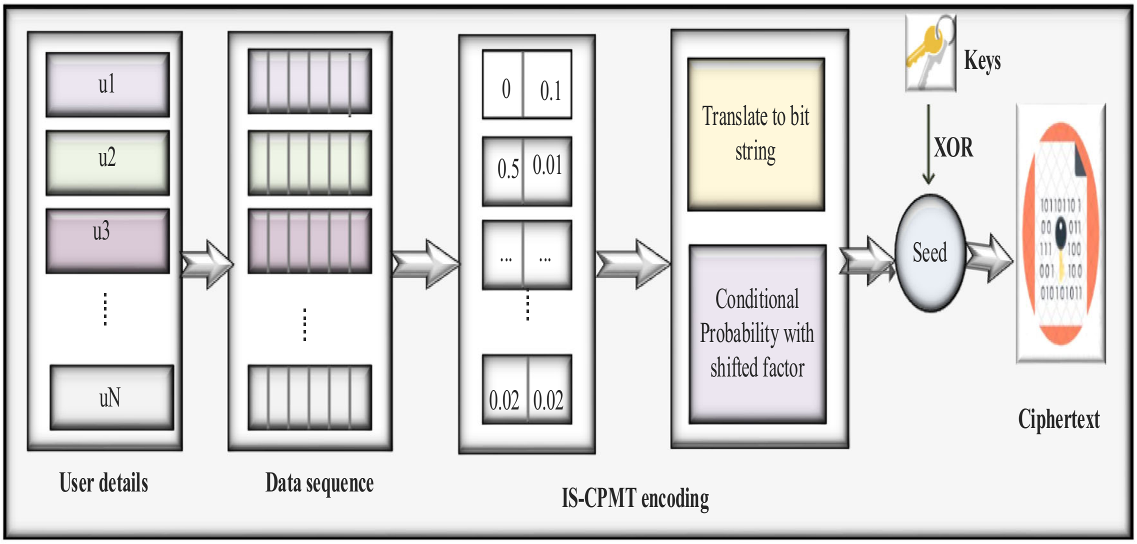


Fig. 5 Process involved in IS-CPMT

carried out to extract the seed *G*. Then, *G* is decoded to extract the rules and the bits for padding is neglected. Next, the user details are acquired from the decoded sequence.

Step 3: If u_i is found to match with the user entities stored in *H,* the request made by u_i is considered valid and allowed to proceed to the next step. This is intimated by *ack_message* to u_i.Otherwise, the request is aborted and the user is detached from the system.

Algorithm.3. Login and data access request phase

```
Input : cipher, pub_key, access_req
Output : pri_key of $dev_i$

procedure D_login (cipher, pub_key, access_req)
verify UC with H,
      extract G
      obtain $ud_1, ud_2, ..ud_x$
        if $u_i = H$, then
            return valid
        else
            reject
      return ack_mesage
    end
end procedure
```

D. Authentication and Session Key agreement phase

Authentication is the process through which the identities of the entities participating in the system are verified and thus enable them to take part in the smart access of devices in the smart home. When the login is successful, the user is confirmed with the system, authentication is carried out in the system with the registered user for attaining services from the IoT devices.

Step 1: For this, consider a session key (*sess_key*) which is computed using the two secret parameters such as w_i and o_i, expressed as,

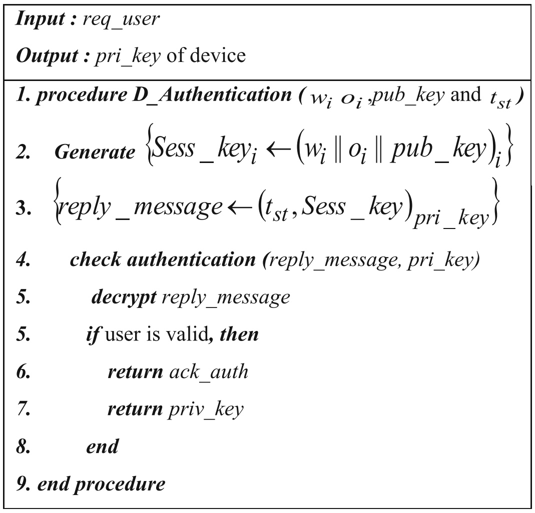
$$\{Sess\_key_i \leftarrow (w_i||o_i||pub\_key)_i\} \tag{6}$$

Step 2: SG issues a timestamp (t_{st}) and the *sess_key* encrypted using *pub_key* of the user to every requesting user ($u_1, u_2, ..u_x$) and to get authenticated to the system for utilizing the services offered by the IoT devices.

Step 3: Every user in the system receives t_{st} and sends a response to the *SG* after decrypting the *sess_key* by their own *pub_key* with the $\{reply\_message \leftarrow (t_{st}, Sess\_key)_{pri\_key}\}$ encrypted by their own private key. Then, *SG* transfers the message to *H* and it verifies the timestamp by decrypting the *reply_message* using *pri_key* of the user and checks for legitimacy. If it is found to be valid the user is allowed to get authenticated to the system. This is indicated by a *ack_auth* message to the user.

Step 4: pri_key of the device is sent to *req_user* for getting access over the device and enables monitoring from remote instance.

Algorithm.4. ***Authentication and session key agreement***



```
Input : req_user
Output : pri_key of device
procedure D_Authentication ( $w_i$ $o_i$ ,pub_key and $t_{st}$ )
  Generate $\{Sess\_key_i \leftarrow (w_i \| o_i \| pub\_key)_i\}$
  $\{reply\_message \leftarrow (t_{st}, Sess\_key)_{pri\_key}\}$
    check authentication (reply_message, pri_key)
      decrypt reply_message
    if user is valid, then
      return ack_auth
      return priv_key
    end
end procedure
```

E. Key updating phase

In this phase, only legitimate users are allowed to participate in the process. Here, the pre-shared key and the secret key are vital for the update of the key. The key update is carried out in a user-friendly manner since u can directly approach the *SG* to make alterations in its key. The system allows faster verification of the user entities and ensures the secure change of the keys.

Step 1: For the key update process, any registered user $(u_1, u_2, ..u_x)$ in the system can login to the system and change his/her secret keys by sending a *chang_key* message to the *SG.*

Step 2: The legitimacy of the user is verified such that input u_x matches with the value of u_x stored in *H*. If matching is genuine, user can modify the keys by choosing their own secret parameter required in the generation of the keys.

The process flow of the proposed MHE-IS-CPMT is shown in Fig. 6.

5 Security analysis

The capability of the proposed system to withstand the attacks from its environment is listed as follows.

Proposition 1 *MHE-IS-CPMT is resistive against a replay attack.*

Proof In this attack, the adversary may try to occur the session key to gain access over the device. Considering this attack, the authentication and key agreement mechanism require the time stamp validity in order to get access to a device present in *H*. Here, the *Sess_key* is sent to the user after encrypting the time stamp with the user's *pub_key.* The user receives the message and decrypts the message and gain the *Sess_key* and time stamp. Then, the reply is sent to *H* by encrypting the *Sess_key* and time stamp with the user's own *pri_key.* When an adversary tries to gain access over the device fails in such a case since the system needs to encrypt the *reply_message* with their own *pri_key.*

Proposition 2 *The proposed scheme is more resilient to impersonation attacks from the mobile user.*

Proof In such attacks, an adversary β tries to register himself as a legitimate user u_β dynamically during runtime. In such a case, the adversary submits its own fake *u_id* and *pw_user* to *SG. H* verifies the user credentials before enabling user registration. When the verification outputs a counterfeit result, *H* marks β as an adversary but issues the *cipher*. Therefore, if β struggles to gain access to the devices, *H* makes a tragic play on the user by issuing a plausible data similar to the original data. This diverts β from the system and hence prevents the leakage of the original data.

Proposition 3 *The proposed scheme is safeguarded from the eavesdropping attack.*

Eavesdropping attack: An adversary β tries to find the secret parameters of u_i and compute the keys to get access over the devices. In this case, the proposed scheme generates the keys for authentication using this parameter. Therefore, it is vital that the generation of the secret parameter must be trustworthy in the system. This smart home system incorporates the ASCII encoding mechanism that chooses at random the bits of the *pw_user* to establish secure generation of e_{u_i}. This makes it tedious for the intruder to compute the secret parameter used in the key generation process. Hence, our system is resilient to this type of attack by adversaries.

Proposition 4 *The proposed scheme is sheltered from the Man-in-the-middle attack.*

Proof To initiate this attack, β intercepts the *reply_message* sent by the user u_i to *SG* in order to get access over the device. In our scheme, the users are authenticated to the system and acquire the *pri_key* earlier. During the device access process, the user encrypts the *Sess_key* with his/her *pri_key* which is unknown to β or any external person. Therefore, it is impossible for β to indulge the message transmitted by u_i. Hence, the contents cannot be modified in any circumstances and thus enabling secure access control features.

Proposition 5 *The user relishes anonymity in the system and the system assures un-traceability.*

Proof In any circumstances β tries to acquire the timestamp t_{st} to get authenticated and gain access over the

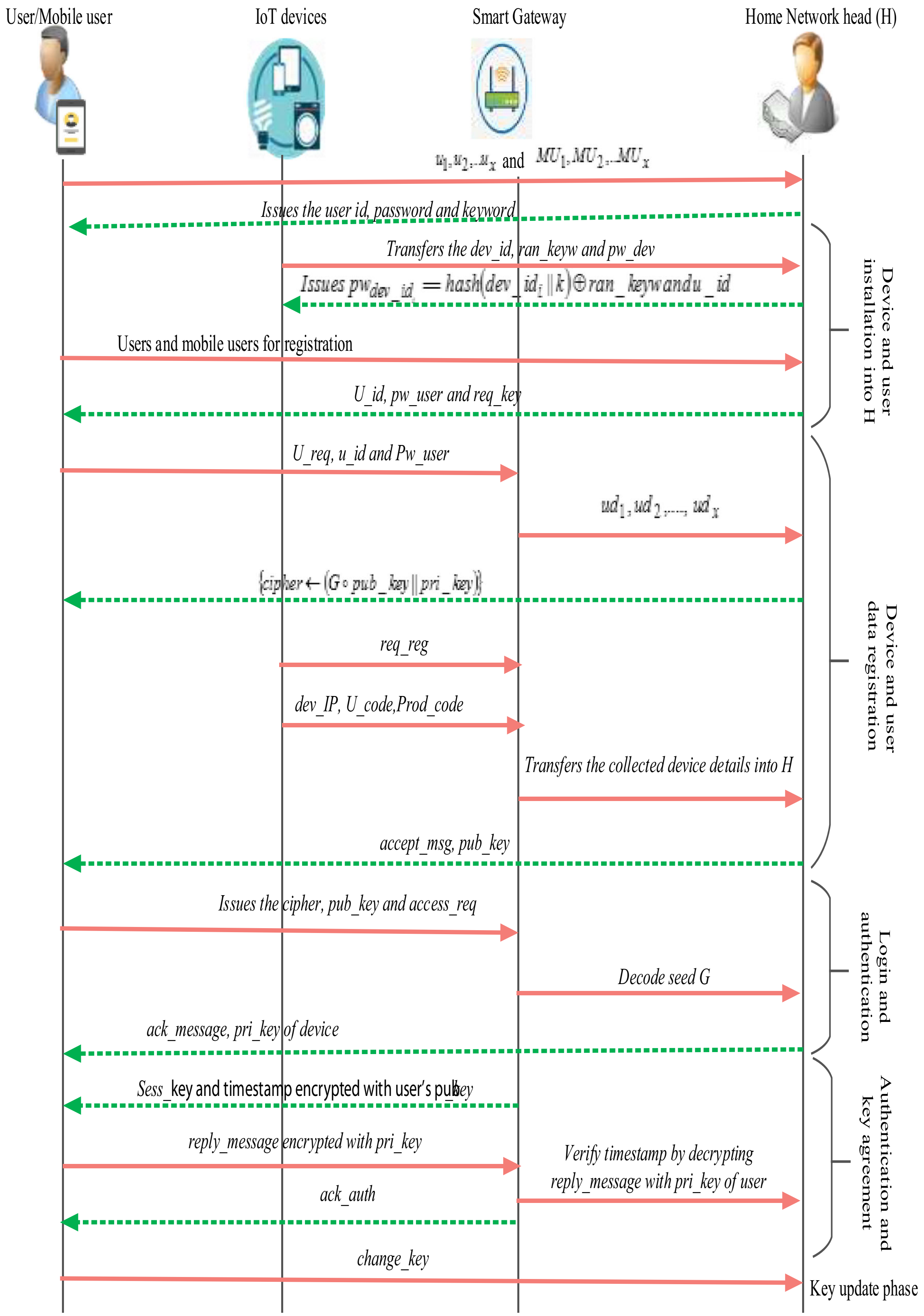

User/Mobile user
IoT devices
Smart Gateway
Home Network head (H)
$u_1, u_2, ..u_x$ and $MU_1, MU_2, ..MU_x$
Issues the user id, password and keyword
Transfers the dev_id, ran_keyw and pw_dev
Issues $pw_{dev\_id_i} = hash(dev\_id_i \| k) \oplus ran\_keyw and u\_id$
Users and mobile users for registration
U_id, pw_user and req_key
Device and user installation into H
U_req, u_id and Pw_user
$ud_1, ud_2, ..., ud_x$
$\{cipher \leftarrow (G \circ pub\_key \| pri\_key)\}$
req_reg
dev_IP, U_code,Prod_code
Transfers the collected device details into H
accept_msg, pub_key
Device and user data registration
Issues the cipher, pub_key and access_req
Decode seed G
ack_message, pri_key of device
Login and authentication
Sess_key and timestamp encrypted with user's pubkey
reply_message encrypted with pri_key
Verify timestamp by decrypting reply_message with pri_key of user
ack_auth
Authentication and key agreement
change_key
Key update phase

Fig. 6 Process flow of MHE-IS-CPMT

devices. Under such requirements the proposed system is robust enough to withstand the impact of β into the system. For this, the system generates inimitable timestamp and the *Sess_key* for every device activation and access control. Moreover, the secret parameters required for the computation of *Sess_key* is altered during every sessions. Due to this unique nature, the proposed system is said to preserve the properties of anonymity and un-traceability.

Proposition 6 *The proposed scheme is resistant to the de-synchronization or jamming attacks.*

Proof This sort of attack is committed by β when the system involves two parties such as the users and the home network head *H*. When the synchronism between these two entities is lost, it is more prone to the attack and the link between them is lost. To deal with this attack, *H* does not store any of the verifications information of the user participating in access. Whenever, the authentication process fails due to the corruption of links, still the system is capable of initiating the system. This is performed by the computation of the secret parameters o_i, w_i without the requirement to re-authenticate to the system.

Proposition 7 *The proposed scheme ensures the properties of the session key agreement.*

Proof The session key agreement is the confidential part for the user without any compromise with the adversary. In this, any adversary β indulges in fraudulent activities to acquire the Sess_key for gaining over the access control process. To fight back against this attack, the proposed scheme reveals the key only to every registered u_i after the finish of the login, authentication and key agreement process. The Sess_key is issued to the user only after initiating the session with a request message access_request. The SG receives the message and makes the devices ready for future communication with the user.

Proposition 8 *MHE-IS-CPMT commits resilience to the Denial-of-Service (DoS) attack.*

Proof Any legitimate user u_i pass in inappropriate *u_id* and *pw_user* to *SG*. These details are verified before allowing the user to login to the system. Therefore, the request of the user to get services is proceeded to further stages only when the user details provided are appropriate. In this way the DoS attack by other adversaries is discarded in the system.

6 Experimental results and analysis

This section presents the efficiency of the proposed approach based on experimental settings, performance metrics, and performance comparison results. These details are described in the following sub-sections.

6.1 Experimental settings

The key agreement based device access control in IoT is carried out using the Python tool. The hardware setup required for the implementation is CPU based computer system with 8 GB, 2 GHz Intel Core i7, and 256 GB memory. The simulation software is taken from the available open-source libraries/packages. Library functions like TensorFlow (TF) is an open source software library used for the IoT simulation platform [39, 40]. TF is the second-generation framework of Google Brain. On Feb 11, 2017, edition 1.0.0 was published. TF, unlike the standard version, can run on many Multi-Core CPUs. It is compatible with 64-bit Linux, macOS, Vista, and smart phones devices such as iOS and android. Its adaptable design enables simple computing deployments over a wide diverse array of substrates from PCs to hundreds of computers to smartphones and other devices. TF allows developers to create a dataflow structure that describes how data moves and the mathematically operations should be done on data during its transfer from one point to another in the defined structure. In this, structure data is presented as tensors and the mathematical operations as nodes. In this, the TF is free and is supported on Python versions for high-performance numerical computation using dataflow graphs. The software tool versions are: Python 3.6 TensorFlow 1.4 [41, 42]. Consider that the each user initiates the communication with the device and perform access for every five seconds. In the experimental tests, the effect of simulation time is observed when the data is transmitted between the user and devices as the number of exchanged bits is increased per unit time. Here six users have been considered out of which two users are mobile and four users are static. The simulation parameters used for the implementation of the smart home system are shown in Table 3.

6.2 Performance metrics

The parameters considered for the evaluation of the proposed scheme involves the End-to-End Delay (EED), throughput, communication cost, computation cost, encryption time and decryption time.

(i) *End to End Delay (EED):* It is defined as the amount of time needed for users to access the system devices. In the authentication and the key agreement process, the EED value is vital for the session key establishment between the user and the *H*. The mathematical expression is denoted as,

$$\sum\nolimits_{i=1}^{n} (t_{rec} - t_{sen})/t_{req} \tag{7}$$

where t_{rec} is the time taken to receive the data corresponding to the request sent, t_{sen} is the time taken to send a request to the *SG*, and t_{req} is the total number of requests sent to *SG*.

Table 3 Parameters for simulation

Parameters	Description
Simulation platform	Python 3.6
Hardware setup	CPU: 8 GB, 2 GHz Intel Core i7, and 256 GB memory
Library function	TensorFlow 1.4
Computing deployments	64-bit Linux, macOS, Vista, and smart phones devices such as iOS and android
Area of deployment	500 m × 500 m
Number of *SG*	4
Total number of users	6
Mobile users	2
Static users	4
Number of devices	20, 40, 60
Communication range of *H*	250 m
Communication time between user and device access	5 s
Communication range of devices	25 m
Considered simulation time	2000 s

(ii) *Throughput:* It calculates the amount of data flow rate transmitted successfully from one entity to another within a given time period. Here, it is measured in bits per second (bps). The mathematical expression is repsrented as,

$$\left(n_d \times s_p\right)/t \tag{8}$$

where n_d is the total number of data accessed from the devices, s_p is the size of the data and t is the total time required to access data from the H.

(iii) *Encryption and Decryption Time:* The amount of time needed to transform plaintext into ciphertext is called the encryption time. In contrast, decryption time restores the plaintext from the received ciphertext.

(iv) *Communication Cost:* It is defined as the ratio of total number of exchanged messages to the total number of exchanged bits for each transaction. Here, it is measured in time (ms).

(v) *Computation Cost:* It is defined as the total amount of validations needed to complete each transaction on the IoT based smart home network. Here, it is measured in milliseconds (ms).

6.3 Performance comparison results

This section presents the comprehensive comparative analysis of the proposed MHE-IS-CPMT scheme is compared with existing methods such as Li et al. [43], Li et al. [44], Srinivas et al. [45], Park et al. [46], Mallareddy et al. [47], Rawal et al. [48], Bogos et al. [49], Shahid et al. [35], Yang et al. [50], Tan et al. [51], Cai et al. [52], Gope et al. [53], Cho et al. [54], and Mansoor et al. [34] in terms of end to end delay, throughput, communication cost, computation cost, time complexity, encryption time and decryption time.

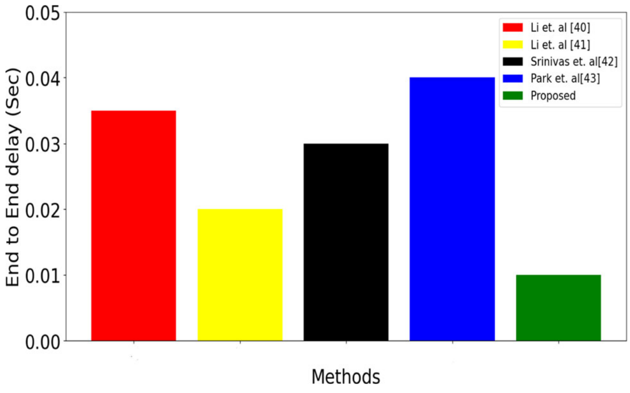


Fig. 7 Comparison results of end to end delay

6.3.1 End to end delay

As shown in Fig. 7, the proposed method achieves a lower end-to-end delay than the Li et al. [43], Li et al. [44], Srinivas et al. [45], Park et al. [46] approaches. Here, the interactional capability of the users with the smart systems is improved to a great extent by the incorporation of the MHE-IS-CPMT scheme. Following this process, users and devices data are securely transmitted with less delay. Therefore, the delay achieved between the users and the device is much lower. Thus, the system achieves better functionality in a limited time interval.

6.3.2 Throughput

Within the considered simulation time, the throughput values are calculated as the number of packet sizes that are transmitted in the network. Existing methods such as Li et al. [43], Li et al. [44], Srinivas et al. [45], Park et al. [46] have lower throughput when the data is transmitted between the user and devices as the number of exchanged bits is increased per unit time. Using the proposed scheme, the number of exchanged messages is increased with higher data security for different network scenarios. As shown in the Fig. 8, the throughput value is higher than the other existing approaches and hence possesses the ability to provide better results for secure data access in smart home networks.

6.3.3 Encryption and decryption time

As shown in Fig. 9a, the proposed MHE-IS-CPMT scheme obtains less encryption time than four approaches,

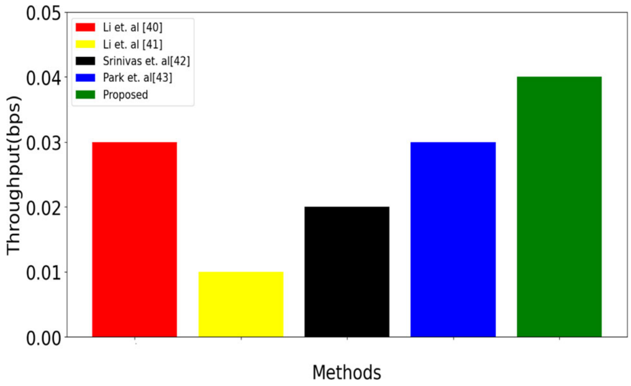


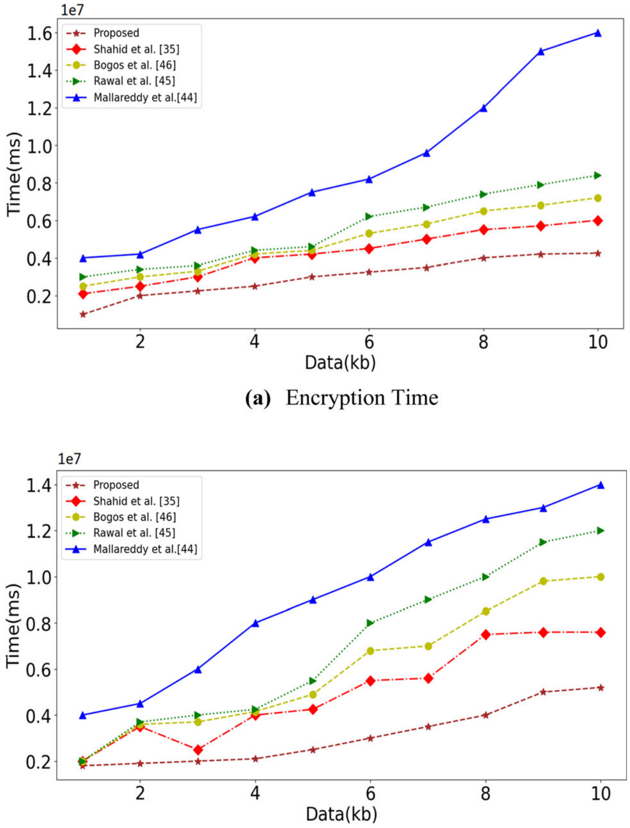
Fig. 8 Comparison results of throughput

Mallareddy et al. [47], Rawal et al. [48], Bogos et al. [49], Shahid et al. [35]. For the existing four techniques, the size of the input data (Kilobytes (Kb)) were similar to the proposed model. Here the time is measured in milliseconds (ms). In the same case of four techniques, the encryption time is increased when the data size is 2 to 10 Kb. This means that the four techniques has the highest encryption time and does not provide data security due to vulnerable attacks. The Fig. 9a observes that the proposed scheme encryption process is done by MHE to encrypt the user and device data. Thus, it can be concluded that the proposed scheme obtains higher security with less encryption time.

In Fig. 9b, the decryption time measures the data confidentiality for the proposed MHE-IS-CPMT scheme and existing four approaches, Mallareddy et al. [47], Rawal et al. [48], Bogos et al. [49], Shahid et al. [35]. In these existing four approaches, the decryption time is increased when the data size large (4 to 8 Kb). Hence the Figure concluded that the proposed approach obtains higher data confidentiality with less decryption time when the data size is large.

6.3.4 Cost complexity analysis

6.3.4.1 Communication cost For communication cost analysis, several parameters are considered such as Authentication tag $Msg(T)$, smart gateway (SG) and home network head (H). In the proposed model, three main entities are considered: User/ mobile user, SG, H. Msg to SG carrying 455 bits and receives 412 bits from SG. At the same time, SG transmits 757 bits and receives 435 bits from H, when H transmits 455 bits and received 757 bits. In terms of communication cost, the proposed model performs secure data transaction among number of bits exchanged in the network.



(a) Encryption Time

(b) Decryption Time

Fig. 9 a and b Comparison results of encryption and decryption time

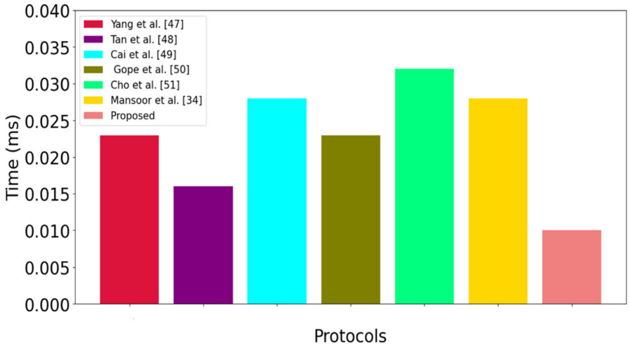


Fig. 10 Comparison results of communication cost

As shown in Fig. 10, the communication cost is performed between the proposed and existing methods. The method presented in Tan et al. [51] has higher communication costs when compared to Yang et al. [50], Cai et al. [52], Gope et al. [53], Cho et al. [54], Mansoor et al. [34] models. The figure observes that the proposed MHE-IS-CPMT scheme achieves lower communication cost than other methods. Thus the proposed model only provides robust security.

6.3.4.2 Computation cost For computation cost analysis, some notations are presented as follows:

- C_c: Computation cost;
- H_f: Security function of C_c;
- $T_{E/D}$: Encryption/Decryption of C_c.

In this experiment, the computation cost is performed on Intel dual-core Pentium processor with specifications of 2 GHz Intel Core i7 processor, 8 GB, and 256 GB memory, respectively. As shown in Fig. 11, the proposed model achieves less computation time of 0.01 ms than existing five methods, Yang et al. [50], Tan et al. [51], Cai et al. [52], Gope et al. [53], Cho et al. [54], Mansoor et al. [34]. For the existing five techniques, the total cost is increased whereas the computation time is also increased as the attackers access the system entities over the communication channel. When compared with these models, the proposed model obtains less computation costs and less running time against different types of attacks. Table 4 shows the analysis of computation cost between the proposed and existing methods in terms of several parameters such as Authentication tag $Msg(T)$, smart gateway (SG) and home network head (H). In comparison with five methods, the total computation cost of proposed model obtains less cost which is equal to 7 H_f + 2 $T_{E/D}$.

6.3.5 Time complexity analysis

Time complexity refers to the time taken to execute every step at the time of simulation. The execution time for every task must be limited within the time budget of the system so as to achieve better performance. Table 5 describes the approximate time required in the computation of several parameters in security functions.

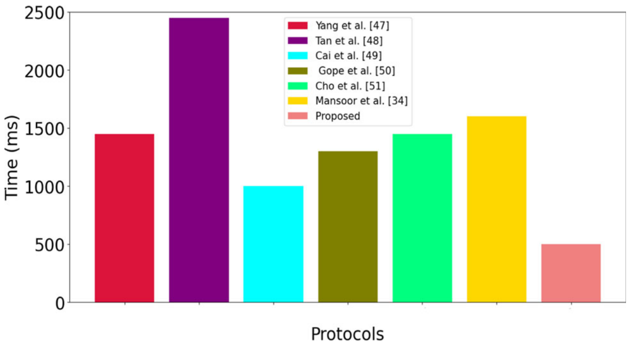


Fig. 11 Comparison results of computation cost

For various entities, the value of each stage is evaluated to find the time complexity of the system. Consider that the total number of transactions for each security level is represented as $n - 1$. The security level of each entity with the longer bits of 1278 provides more security features for the message length of 2. Thus, its time complexity is signed as O (n). Also, the total number of transactions with a time complexity of $O(2^{n-1})$. The time complexity of each entity is shown in the Table 6.

6.3.6 Security features analysis

The expected security features ensures secure authentication and data access using proposed MHE-IS-CPMT scheme. The list of security features is compared with the existing methods and proposed method are as follows:

SF1: Mutual authentication
SF2: Un-traceability
SF3: User anonymity
SF4: Session key agreement
SF5: Eavesdropping attack
SF6: Home gateway impersonation attack
SF7: Replay attack
SF8: Man-in-the-middle attack
SF9: Jamming attacks
SF10: Denial-of-Service (DoS) attack

Table 7 shows the comparison results of security features (SF1 to SF10) between the proposed and existing methods.

The security feature comparison of proposed and existing methods is shown in Table. Both the schemes by Yang et al. [50] and Tan et al. [51] does not provide mutual authentication, un-traceability and user anonymity and cannot resist eavesdropping attack and home gateway impersonation attack. The scheme by Cai et al. [52] does not provide session key agreement, eavesdropping attack and un-traceability and the method presented in Gope et al.

Table 4 Comparison results of computation time and cost

C_c	Yang et al. [50]	Tan et al. [51]	Cai et al. [52]	Gope et al. [53]	Cho et al. [54]	Mansoor et al. [34]	Proposed model
C_cT	2 H_f	2 H_f	4 H_f	5 H_f	3 H_f	2 H_f	2 H_f
C_cSG	3 H_f	2 H_f	2 H_f	2 H_f	2 H_f	2 H_f	2 H_f
C_cH	5 H_f	3 H_f	6 H_f	7 H_f	5 H_f	4 H_f + 2 $T_{E/D}$	3 H_f + 2 $T_{E/D}$
C_{cTotal}	10 H_f	7 H_f	12 H_f	14 H_f	10 H_f	8 H_f + 2 $T_{E/D}$	7 H_f + 2 $T_{E/D}$
C_{cTime}	0.02 ms	0.02 ms	0.03 ms	0.02 ms	0.03 ms	0.027 ms	0.01 ms

[53] is vulnerable to home gateway impersonation attack, replay attack and DoS attack. Mansoor et al. [34] obtains more security features but it cannot provide session key agreement, and cannot prevent eavesdropping attack, home gateway impersonation attack and man-in-the-middle attack. From the overall results, the proposed MHE-IS-CPMT scheme achieves all security features than existing methods.

7 Research limitations

In this research work, there are some limitations of the proposed model, which are mentioned as follows: (1) ensuring the security of smart home systems between the information exchange of IoT devices and the server is robust, but the proposed model does not focus on the computing power of IoT devices, (2) the proposed work primarily focuses on user authentication based on the daily access time to smart home devices. However, most online devices are highly dependent on networks, so offline devices can redirect user access patterns to be incorrect. (3) Unified data access is possible, but our proposed model does not support hardware compatibility on some devices.

Table 5 Computation time for security parameters

Notation	Description (time taken for computation)	Approximate time for computation (seconds)
$t_{pw_{dev\_id}}$	Password generation	0.00021
t_{key}	Key generation	0.00712
t_{HE}	Honey based encryption	0.0921
t_{reg}	Registration	0.0035
t_{auth}	Authentication	0.0234

Table 6 Time complexity

Notation	Entities	Time complexity
$t_{reg} + 2t_{pw_{dev\_id}}$	User/mobile user	0.00042
$5t_{key} + t_{reg}$	*SG*	0.0391
$2t_{auth} + 2t_{reg} + 2t_{HE}$	*H*	0.19588
	Total time	0.2354

8 Conclusion

In this paper, the MHE-IS-CPMT is proposed for secure authentication and key agreement between the users and devices participating in the smart home system. The initialized users and devices of the network are allowed to register into the system. Then, only the registered users are allowed to access and control the devices of the smart home and gain access to the sensitive data. Further, if any adversaries attack the system, the protocol sends plausible responses to confuse the adversaries present in the system. Also, the system model is designed such that it is more resilient to different type of attacks. Finally, the performance results is evaluated that the capability of the system obtains more security features in comparison with other existing approaches. Also, the proposed MHE-IS-CPMT scheme demonstrates that the comparative analysis results obtains best results in terms of end to end delay, communication cost, throughput, computation cost, time complexity, encryption time and decryption time. From the experimental results, the proposed model achieves a lower computation time of 0.01 ms and more security features than existing methods in the secure data transfer of the IoT smart home system.

Table 7 Comparison of security features between the proposed and existing methods (✔: fully covered and mentioned and x: not mentioned)

Security features (SF)	Yang et al. [50]	Tan et al. [51]	Cai et al. [52]	Gope et al. [53]	Cho et al. [54]	Mansoor et al. [34]	Proposed model
SF1	x	x	✔	✔	✔	✔	✔
SF2	x	x	x	✔	✔	✔	✔
SF3	x	x	✔	✔	x	✔	✔
SF4	x	✔	x	✔	✔	x	✔
SF5	x	x	x	✔	x	x	✔
SF6	x	x	x	x	✔	x	✔
SF7	✔	✔	✔	x	✔	✔	✔
SF8	✔	✔	✔	✔	✔	x	✔
SF9	✔	✔	✔	✔	✔	✔	✔
SF10	✔	✔	✔	x	✔	✔	✔

Authors' contributions All the authors have participated in writing the manuscript and have revised the final version. All authors read and approved the final manuscript.

Declarations

Conflict of interest Authors declares that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants and/or animals performed by any of the authors.

Informed consent There is no informed consent for this study.

References

1. Chakraborty, S., Bhatt, V., & Chakravorty, T. (2019). Impact of IoT adoption on agility and flexibility of healthcare organization. *International Journal of Innovative Technology and Exploring Engineering, 8*(11), 2673–2681. https://doi.org/10.35940/ijitee.k2119.0981119
2. Alvi, S. A., Afzal, B., Shah, G. A., Atzori, L., & Mahmood, W. (2015). Internet of multimedia things: Vision and challenges. *Ad Hoc Networks, 33*, 87–111. https://doi.org/10.1016/j.adhoc.2015.04.006
3. Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). Cyber security threats to IoT applications and service domains. *Wireless Personal Communications, 95*(1), 169–185. https://doi.org/10.1007/s11277-017-4434-6
4. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010
5. Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications, 97*, 48–65. https://doi.org/10.1016/j.jnca.2017.08.017
6. Jaikla, T., Vorakulpipat, C., Rattanalerdnusorn, E., & Hai, H. D. (2019). A secure network architecture for heterogeneous iot devices using role-based access control. In *2019 International conference on software, telecommunications and computer networks (SoftCOM)* (pp. 1–5). IEEE. https://doi.org/10.23919/softcom.2019.8903605
7. Togan, M., Chifor, B. C., Florea, I., & Gugulea, G. (2017). A smart-phone based privacy-preserving security framework for IoT devices. In *2017 9th International conference on electronics, computers and artificial intelligence (ECAI)* (pp. 1–7). IEEE. https://doi.org/10.1109/ecai.2017.8166453
8. Beitollahi, H., & Deconinck, G. (2012). Analyzing well-known countermeasures against distributed denial of service attacks. *Computer Communications, 35*(11), 1312–1332. https://doi.org/10.1016/j.comcom.2012.04.008
9. Sciancalepore, S., Piro, G., Boggia, G., & Bianchi, G. (2016). Public key authentication and key agreement in IoT devices with minimal airtime consumption. *IEEE Embedded Systems Letters, 9*(1), 1–4. https://doi.org/10.1109/les.2016.2630729
10. Atamli, A. W., & Martin, A. (2014). Threat-based security analysis for the internet of things. In *2014 International workshop on secure internet of things* (pp. 35–43). IEEE. https://doi.org/10.1109/siot.2014.10
11. Chen, B., Huang, Y. L., & Güneş, M. (2015). S-CBAC: A secure access control model supporting group access for Internet of Things. In *2015 IEEE International symposium on software reliability engineering workshops (ISSREW)* (pp. 67–67). IEEE. https://doi.org/10.1109/issrew.2015.7392046
12. Rivera, D., Cruz-Piris, L., Lopez-Civera, G., de la Hoz, E., & Marsa-Maestre, I. (2015). Applying an unified access control for IoT-based intelligent agent systems. In *2015 IEEE 8th international conference on service-oriented computing and applications (SOCA)* IEEE, 247–251. https://doi.org/10.1109/soca.2015.40
13. Li, J., Chen, X., Li, J., Jia, C., Ma, J., & Lou, W. (2013). Fine-grained access control system based on outsourced attribute-based encryption. In *European symposium on research in computer security* (pp. 592–609). Springer. https://doi.org/10.1016/j.jss.2016.12.018
14. Wang, H., He, D., Shen, J., Zheng, Z., Zhao, C., & Zhao, M. (2017). Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing. *Soft Computing, 21*(24), 7325–7335. https://doi.org/10.3837/tiis.2017.06.024
15. Gaikwad, P. P., Gabhane, J. P., & Golait, S. S. (2015). 3-level secure Kerberos authentication for smart home systems using IoT. In *2015 1st International conference on next generation computing technologies (NGCT)* (pp. 262–268). IEEE. https://doi.org/10.1109/ngct.2015.7375123
16. Mahalle, P. N., Prasad, N. R., & Prasad, R. (2014). Threshold cryptography-based group authentication (TCGA) scheme for the Internet of Things (IoT). In *2014 4th International conference on wireless communications, vehicular technology, information theory and aerospace and electronic systems (VITAE)* (pp. 1–5). IEEE. https://doi.org/10.1109/vitae.2014.6934425
17. Forsby, F., Furuhed, M., Papadimitratos, P., & Raza, S. (2017). Lightweight x. 509 digital certificates for the internet of things. In *Interoperability, safety and security in IoT* (pp. 123–133). Springer. https://doi.org/10.1007/978-3-319-93797-7_14
18. Gyamfi, E., Ansere, J. A., & Xu, L. (2019). ECC based lightweight cybersecurity solution for IoT networks utilising multi-access mobile edge computing. In *2019 Fourth international conference on fog and mobile edge computing (FMEC)* (pp. 149–154). IEEE. https://doi.org/10.1109/fmec.2019.8795315
19. Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A. R., & Tarkoma, S. (2017). Iot sentinel: Automated device-type identification for security enforcement in iot. In *2017 IEEE 37th international conference on distributed computing systems (ICDCS)* (pp. 2177–2184). IEEE. https://doi.org/10.1109/icdcs.2017.283
20. Hao, P., Wang, X., & Shen, W. (2018). A collaborative PHY-aided technique for end-to-end IoT device authentication. *IEEE Access, 6*, 42279–42293. https://doi.org/10.1109/access.2018.2859781
21. Lee, I., & Lee, K. (2015). The internet of things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008
22. Hossain, M.M., Fotouhi, M., & Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. In*2015 IEEE world congress on services*. IEEE, 21–28. https://doi.org/10.1109/services.2015.12
23. Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing., 1*, 8. https://doi.org/10.1007/s12652-017-0494-4
24. Alassaf, N., Gutub, A., Parah, S. A., & Al Ghamdi, M. (2019). Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimedia Tools and Applications., 78*(23), 32633–32657. https://doi.org/10.1007/s11042-018-6801-z
25. Tewari, A., & Gupta, B. B. (2017). Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using

RFID tags. *The Journal of Supercomputing., 73*(3), 1085–1102. https://doi.org/10.1007/s11227-016-1849-x

26. Chifor, B. C., Bica, I., Patriciu, V. V., & Pop, F. (2018). A security authorization scheme for smart home Internet of Things devices. *Future Generation Computer Systems, 86*, 740–749. https://doi.org/10.1016/j.future.2017.05.048
27. Shen, J., Wang, C., Li, T., Chen, X., Huang, X., & Zhan, Z. H. (2018). Secure data uploading scheme for a smart home system. *Information Sciences, 453*, 186–197. https://doi.org/10.1016/j.ins.2018.04.048
28. Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., & Burnap, P. (2019). A supervised intrusion detection system for smart home IoT devices. *IEEE Internet of Things Journal, 6*(5), 9042–9053. https://doi.org/10.1109/jiot.2019.2926365
29. Yan, H., Wang, Y., Jia, C., Li, J., Xiang, Y., & Pedrycz, W. (2019). IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT. *Future Generation Computer Systems, 95*, 344–353. https://doi.org/10.1016/j.future.2018.12.061
30. Alshahrani, M., & Traore, I. (2019). Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain. *Journal of Information Security and Applications, 45*, 156–175. https://doi.org/10.1016/j.jisa.2019.02.003
31. Punithavathi, P., Geetha, S., Karuppiah, M., Islam, S. H., Hassan, M. M., & Choo, K. K. R. (2019). A lightweight machine learning-based authentication framework for smart IoT devices. *Information Sciences, 484*, 255–268. https://doi.org/10.1016/j.ins.2019.01.073
32. Naik, K., & Patel, S. (2018). An open source smart home management system based on IOT. *Wireless Networks*. https://doi.org/10.1007/s11276-018-1884-z
33. Gochhayat, S. P., Lal, C., Sharma, L., Sharma, D. P., Gupta, D., Saucedo, J. A., & Kose, U. (2020). Reliable and secure data transfer in IoT networks. *Wireless Networks, 26*(8), 5689–5702. https://doi.org/10.1007/s11276-019-02036-0
34. Mansoor, K., Ghani, A., Chaudhry, S. A., Shamshirband, S., Ghayyur, S. A., & Mosavi, A. (2019). Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography. *Sensors, 19*(21), 4752. https://doi.org/10.3390/s19214752
35. Shahid, F., Ashraf, H., Ghani, A., Ghayyur, S. A., Shamshirband, S., & Salwana, E. (2020). PSDS–proficient security over distributed storage: A method for data transmission in cloud. *IEEE Access, 8*, 118285–118298. https://doi.org/10.1109/access.2020.3004433
36. Samuel, O., Omojo, A. B., Onuja, A. M., Sunday, Y., Tiwari, P., Gupta, D., Hafeez, G., Yahaya, A. S., Fatoba, O. J., & Shamshirband, S. (2022). IoMT A COVID-19 healthcare system driven by federated learning and blockchain. *IEEE Journal of Biomedical and Health Informatics, 1*, 21. https://doi.org/10.1109/jbhi.2022.3143576
37. Jaeger, J., Ristenpart, T., & Tang, Q. (2016). Honey encryption beyond message recovery security. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 758–788). Springer. https://doi.org/10.1007/978-3-662-49890-3_29
38. Santoso, F. K., & Vun, N. C. (2015). Securing IoT for smart home system. In *2015 international symposium on consumer electronics (ISCE)* (pp. 1–2). IEEE. https://doi.org/10.1109/isce.2015.7177843
39. https://www.tensorflow.org/about/bib
40. Sarawale, R., Deshpande, A., & Arora, P. (2021). Implementation pathways of smart home by exploiting internet of things (IoT) and Tensorflow. In *Data science and security* (pp. 478–489), Springer.
41. Nagpal, A., & Gabrani, G. (2019). Python for data analytics, scientific and technical applications. In *2019 Amity international conference on artificial intelligence (AICAI)* (pp. 140–145). IEEE. https://doi.org/10.1109/aicai.2019.8701341
42. https://www.python.org/downloads/release/python-368/
43. Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A. K., & Choo, K. K. R. (2018). A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. *Journal of Network and Computer Applications, 103*, 194–204. https://doi.org/10.1016/j.jnca.2017.07.001
44. Li, X., Niu, J., Bhuiyan, M. Z. A., Wu, F., Karuppiah, M., & Kumari, S. (2017). A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things. *IEEE Transactions on Industrial Informatics, 14*(8), 3599–3609. https://doi.org/10.1109/tii.2017.2773666
45. Srinivas, J., Das, A. K., Wazid, M., & Kumar, N. (2018). Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things. *IEEE Transactions on Dependable and Secure Computing, 17*(6), 1133–1146. https://doi.org/10.1109/tdsc.2018.2857811
46. Park, K., Noh, S., Lee, H., Das, A. K., Kim, M., Park, Y., & Wazid, M. (2020). LAKS-NVT: Provably secure and lightweight authentication and key agreement scheme without verification table in medical internet of things. *IEEE Access, 8*, 119387–119404. https://doi.org/10.1109/access.2020.3005592
47. Mallareddy, A., Bhargavi, V., & Rani, K. D. (2014). A single to multi-cloud security based on secret sharing algorithm. *International Journal of Research, 1*(7), 910–915. https://doi.org/10.15373/22501991/mar2013/35
48. Rawal, B. S., Vijayakumar, V., Manogaran, G., Varatharajan, R., & Chilamkurti, N. (2018). 'Secure disintegration protocol for privacy preserving cloud storage.' *Wireless Personal Communications, 103*(2), 1161–1177. https://doi.org/10.1007/s11277-018-5284-6
49. Bogos, S., Gaspoz, J., & Vaudenay, S. (2018). Cryptanalysis of a homomorphic encryption scheme. *Cryptography and Communication, 10*(1), 27–39. https://doi.org/10.1109/isit.2012.6283832
50. Yang, J., Park, J., Lee, H., Ren, K., & Kim, K. (2005). Mutual authentication protocol for low-cost RFID. In *Workshop on RFID and lightweight crypto WRLC* (pp. 17–24). https://doi.org/10.1109/apscc.2010.22
51. Tan, C. C., Sheng, B., & Li, Q. (2008). Secure and serverless RFID authentication and search protocols. *IEEE Transactions on Wireless Communications*. https://doi.org/10.1109/twc.2008.061012
52. Cai, S., Li, Y., Li, T., & Deng, R. H. (2009). Attacks and improvements to an RIFD mutual authentication protocol and its extensions. *Proceedings of the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16–19*, 51–58. https://doi.org/10.1145/1514274.1514282
53. Gope, P., & Hwang, T. (2015). A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. *Computers and Security, 55*, 271–280. https://doi.org/10.1016/j.cose.2015.05.004
54. Cho, J. S., Jeong, Y. S., & Park, S. O. (2015). Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol. *Computers and Mathematics with Applications, 69*, 58–65. https://doi.org/10.1016/j.camwa.2012.02.025

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Sirisha Uppuluri received the Masters degree from Jawaharlal Nehru technological university, Hyderabad in 2013. She is currently pursuing Ph.D. (PT) in the GITAM University. She is currently working as Assistant Professor in Narsimha Reddy Engineering College. Her research interests includes the security, internet of things and machine learning

Dr.G. Lakshmeeswari received Ph. D. in Computer Science and Engineering from GITAM Deemed to be University, Visakhapatnam, Andhra Pradesh, India in 2013.She is currently working as Associate Professor in GITAM Deemed to be University. She has more than 20 years of experience in teaching. She published research articles various national and international journals and conferences. Her research areas include Cloud Computing, Security, internet of things and visual cryptography.