



Lightweight authenticated key agreement scheme for Cloud-assisted Internet of Things

Bommepalli Narayana Reddy^{1*}, Dr.B.Raja Koti²

^{1,a}Academic Consultant, GDT Department, DrYSR Architecture and Fine Arts University, Kadapa, AP, India.

^{1,b}Part-time Research Scholar, GITAM University, Visakhapatnam, India.
*nbommepa@gitam.in

² Assistant Professor, CSE Department, GITAM University, Visakhapatnam, A.P, India
rbadugu@gitam.edu

Abstract: Internet of Things (IoT) devices face power constraints, manufacturers increasingly focus on group communication for their applications. Such communication heavily relies on a dependable, efficient, and verifiable group secret key. Blockchain technology has the power to solve the problems because it is decentralized, secure, and private. The Internet of Things poses unique challenges for authentication and key management methods due to resource constraints and placement of constituent devices in places where physical access to the devices is possible. This paper introduces an innovative authenticated key management system for Cloud-Assisted Industrial Internet of Things. The protocol addresses the issue of a single point of failure while preserving the security attributes of the existing system. We propose ways for implementing lightweight authenticated key management schemes that are specifically designed for various design processes. A technique that requires authentication is implemented using elliptic curve and hash algorithms. This scheme also offers the functionality of adding and removing clients, as well as ensuring the freshness of keys. We conducted an empirical investigation using a proposed method and evaluated its performance using the Scyther verification tool. The topics of security analysis and computational complexity have also been addressed. We conclude by outlining potential future research directions.

Keywords: Internet of Things (IoT), Authentication, Key Management, Lightweight Cryptography, Cloud Server, Security.

1. Introduction

Today, there is a significant volume of data generated on a daily basis from a wide range of sources such as health organizations, governments, internet sources, social networks, and the financial sectors. Additionally, data is also generated from the Internet of Things, Cloud Computing, the proliferation of smart devices in various applications, and smart grid systems. Wireless sensor networks (WSNs) consist of multiple self-organized nodes without a central control node. These nodes are capable of multi-hop communication, even if they are outside the transmission range. The Internet of Things (IoT) is a crucial component of upcoming networking technologies. In an ecosystem enabled by the Internet of Things (IoT), physical items or things are no longer characterized by their lack of responsiveness. However, individuals possess access to the Internet and possess the ability to process and exchange information. Wireless sensor networks (WSNs) are essential for the deployment of Internet of Things (IoT) technology. IoT has become a prominent element of modern networking technology in recent years. In an ecosystem enabled by the IoTs physical items or things are no longer characterized by their lack of responsiveness. Conversely, these devices are interconnected with the Internet and equipped with processing and communication functionalities.

Creating a secure group key [9] is essential for maintaining the integrity, authenticity, and confidentiality of message transfers within multicast groups. Furthermore, group key establishment procedures must be able to adapt to the particular characteristics of devices and networks found in Internet of Things (IoT)-enabled Wireless Sensor Networks (WSNs). These attributes include limitations in resources, the capacity to scale effectively, and the capability to construct groups dynamically.

© The Author(s) 2024

K. R. Madhavi et al. (eds.), *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024)*, Advances in Computer Science Research 112,

https://doi.org/10.2991/978-94-6463-471-6_122

The Internet of Things (IoT) is a networked system comprising interconnected electronic devices, machines, animals, persons, and other objects. Every entity is allocated distinct unique identifiers (UIDs) and possesses the capability to independently communicate and share data via a network, without necessitating direct interaction between humans or between humans and computers [21]. The IoT ecosystem consists of a network of interconnected intelligent devices that are equipped with embedded systems, such as CPUs, sensors, and communication hardware. These devices are capable of gathering data from their surroundings, transmitting it, and taking appropriate actions based on the acquired information. Internet of Things (IoT) devices facilitate the sharing of sensor data they gather by establishing connections with an IoT gateway or alternative edge device [3,17]. Subsequently, this data is either transmitted to the cloud for analysis or analyzed on the local device. Figure 1.1 depicts the layered architecture, technology, security challenges, and fundamental security methods associated with the Internet of Things (IoT).

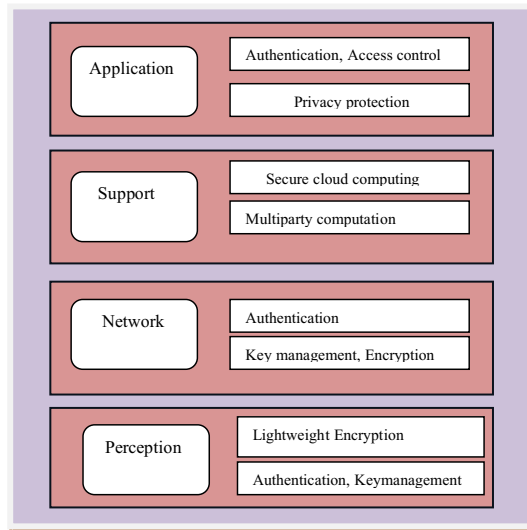


Fig 1: IoT layered architecture

One of the primary security considerations in the suggested protocols is the assurance of message transaction integrity and authenticity. In the evolution of IoT oriented technologies, practical appliances are encountering key elements like - sensing, able to process, as well as communicating the systems [12]. It often relates archetype to provide the comparatively strong data proclamation over the uncertain networks. Resultantly, the IoT prototype computationally inherits the diverse security weaknesses which are frequently formed in the all varieties of cyber-physical systems as well as the Internet .

1.1 System model of Internet of Things (IoT)

The Internet of Things (IoT) is a networked system comprising interconnected electronic devices, machines, animals, persons, and other objects. Every entity is allocated distinct unique identifiers (UIDs) and possesses the capability to independently communicate and share data via a network, without necessitating direct contact between humans or between humans and computers [21]. An IoT ecosystem is a network of interconnected smart devices that have integrated systems, including central processing units (CPUs), sensors, and communication equipment. These gadgets are specifically engineered to collect, transmit, and react to data acquired from their immediate surroundings. IoT devices participate in the exchange of sensor data with an IoT gateway or another edge device. Afterwards, this data is either sent to the cloud for processing or undergoes local scrutiny.

Cloud servers [1,30] are strategically situated in various data centers across the globe. The issue of security in cloud computing is a significant area of concern. It is imperative to ensure that data saved in the cloud is encrypted. In order to prevent clients from directly accessing shared data, it is recommended

to utilize proxy and brokerage services. Cloud computing [2,35,5] in the context of the IoT operates through collaborative mechanisms and serves as a means to store data generated by IoT devices.

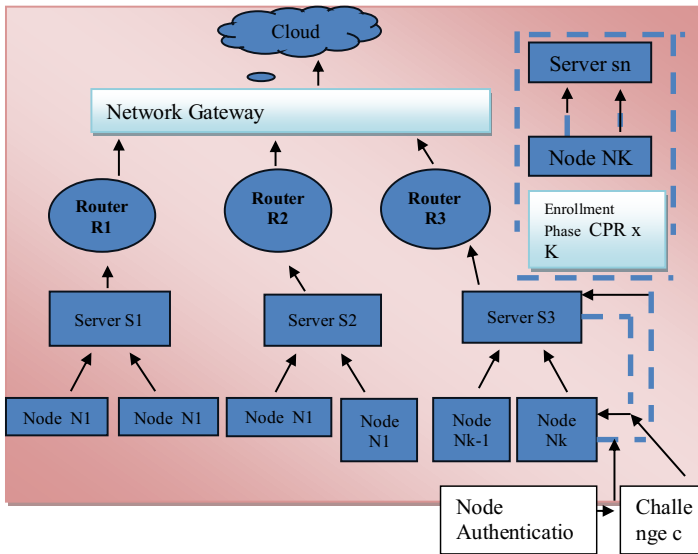


Fig 2. System model of IoT

- i. **Industry 4.0:** The IoT technology connects an array of machines, devices, and systems, allowing them to communicate and exchange information seamlessly within a factory or production facility as part of Industry 4.0, allowing for Instantaneous communication and data sharing
- ii. **Internet of Drones:** In the Internet of Drones (IoD), IoT technology is used to connect drones, allowing for Instantaneous communication and data sharing.
- iii. **Smart homes:** The term "smart homes" or "home automation" pertains to the utilization of IoT technology for the automation and management of various household operations, such as lighting, heating, and security.
- iv. **Healthcare:**The utilization of IoT technology in the healthcare industry, commonly called as the Internet of Medical Things (IoMT), involves the use of IoT devices to improve patient care and the delivery of healthcare services [6,7].
- v. **Smart Grid Network:** A smart grid is an advanced electrical grid that uses IoT technology to communicate and control energy generation, distribution and consumption.
- vi. **Communication Technologies:** Wireless communication technology that is specifically engineered for facilitating low-power, short-range communication among devices. Mobile networks and applications enable remote users to access Internet services at any time and from any location.

2. SECURITY MECHANISMS OF INTERNET OF THINGS

2.1 Authentication Schemes

Authentication [12,13,22] is crucial, particularly for internet businesses. We can authenticate users in a number of methods. Typically, authentication takes place numerous times per day. Organisations must modify their security measures to keep up with the rapid advancement of technology if they want to effectively combat fraudsters, hackers, thieves, and the like. Since the modifications may affect how the service is viewed as being usable, caution must be given when implementing new security protocols[25,26]. This is crucial because customer adoption of security measures depends on their usability; if security processes are challenging to use, customers will avoid them or use them incorrectly.

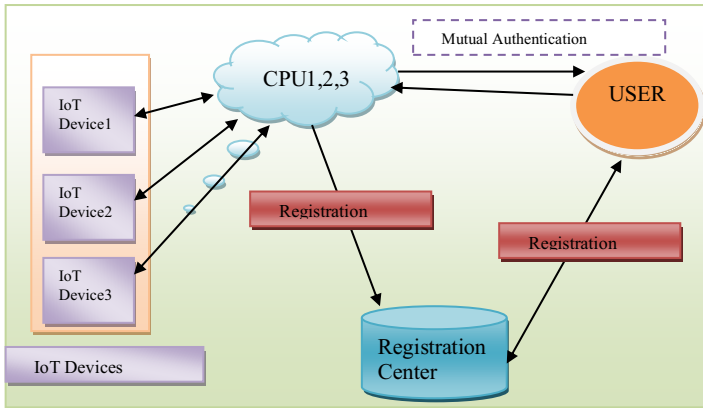


Fig 3. A Secure Authentication for IoT-Based Cloud Computing

2.2 Taxonomy of IoT Authentication Schemes

i. Authentication Factor:

- Identity refers to the information that is provided by one entity to another in order to establish its authenticity. This process can involve the use of various cryptographic algorithms, such as hash functions, symmetric encryption, or asymmetric encryption.
- The context of the situation is as follows: Physical biometric information refers to the collection and analysis of data derived from distinctive physical traits, such as fingerprints and hand shape.
- Behavioral biometrics refers to the use of behavioral features, such as key-stroke dynamics and voice identification, as a means of biometric identification [28,20].

ii. Use of Tokens:

- Token based: based on an identification token.
- Non-token based: involves use of credentials.

iii. Authentication Procedure:

- One approach is a scenario in which only one party undergoes the process of authentication, while the other party remains unauthenticated.
- Mutual authentication is a two-way process in which both entities involved verify each other's identities.
- In three-way authentication method, a central authority plays a crucial role in verifying the identities of both parties involved and facilitating their mutual authentication.

- Hardware Based:** Implicit hardware-based authentication methods leverage the inherent properties of the hardware to enhance the authentication process, for instance, through the utilization of Physical Unclonable Function.

2.3 Key Management Schemes

Key management techniques covered in this section include pair-wise, polynomials-based, master key-based, location-based, and random key distribution. Confidentiality is ensured by ensuring that symmetric algorithms [22] satisfy WSN's requirements for power, area, and memory. Symmetric algorithms provide anonymity while satisfying the power, space, and memory requirements of WSN. Due to the resource and energy limitations of the sensor node, the majority of conventional key management solutions are inappropriate for wireless sensor networks. The benefit of point-to-multipoint (multicast) communication, in which a single source disseminates accurate information to several recipients, ensures that group key management schemes work well. As most of the nodes are distinct in reality, it is difficult to physically or cognitively group them. A distributed IoT environment does not allow this method, despite the fact that a central authority should be in charge of supervising the group [9]. However, creating and managing such a multicast group in the real world, particularly in the IoT environment, requires a lot of time and work.

As IoT-focused technologies improve, practical appliances are beginning to encounter

crucial components including sensors, processing power, and system connectivity [12]. Archetype is commonly associated with providing fairlyreliable data declaration across uncertain networks. Because of this, the Internet of Things prototype computationally inherits all of the security problems that frequently appear in the Internet and all other kinds of cyber-physical systems. The first important security feature of any suggested protocol is its guarantee of the integrity and validity of message transactions.

In investigates the lack of security in IoT devices in relation to the IoT stack provided by standardization groups. It concludes that the data encryption process at the network layer is ineffective and mainly focuses on the physical and data link levels. [11] addresses the problem of establishing a session key between a client and a server in the Internet of Things setting and provides alternative solutions. A comprehensive review of GKM protocols using various key distribution models as classification criteria is presented . The review of synchronous and asynchronous GKM processes demonstrates that the current methodologies either fail to account for reliability mechanisms or fail to apply the mechanisms in the desired dynamically changing limited situation. The substantial amount of airtime needed to exchange messages for key agreement and authentication is addressed in [13] approach. It offers a solution through a cutting-edge key management protocol that performs authentication and key agreement while integrating implicit certificates with a traditional elliptic curve Diffie-Hellman exchange. A Key Management Protocol (KMS) for a Hierarchical IoT network is provided in [9]. It uses three factors for authentication and key generation: a smart card, a password, and biometrics. Investigates the issue of node capture attacks from an adversarial perspective in [21], where the attacker skillfully exploits the flaws. The plan creates a comparable attack matrix in response. This matrix assigns a key dominance rating and identifies a group of crucial nodes. Using group-based keys in a clustered and distributed key management system, [3] offers a solution and techniques for achieving confidentiality and end-to-end guarantees. It uses a clustering strategy to spread the massive IoT network.

A matrix-based approach to key management was established in [22]. The solution utilized encryption to enhance store capacity and reduce the weight of nodes. This strategy enhances the durability of node capture. Furthermore, it provides a greater amount of storage space. If there is a network interruption, the client will have to deal with higher communication overhead. A proposed in [13] presents a specialized authentication and key agreement method designed for Wireless Sensor Networks (WSN) in an Industrial Internet of Things (IIoT) environment. This approach resulted in rapid authentication procedures and an unexpectedly extended period for pseudonym changes. The proposed solutions, known as logical tree-based secure mobility management (LT-SMM), utilizes mobile service computing [53,14]. In order to ensure the integrity of the message, it has employed one-way hash algorithms based on chaotic maps. It alleviates and resolves issues related to redundant data entry. The study [16] presents a scalable multi-group key management protocol specifically intended for the Internet of Things. This protocol ensures both forward and backward secrecy, provides strong protection against collision attacks, and allows for secure coexistence of diverse services. The paper referenced in [18] proposes a technique for achieving mutual authentication and session key agreement, so providing secure communication in Wireless Sensor Networks (WSNs) enabled by the Internet of Things (IoT).The generation of a session key involves the utilization of Weil pairing and Elliptic Curve Cryptography (ECC). The Scheme is safeguarded against replay attacks as the recipient verifies the sent information by examining the nonce.

Table 1: Comparison various our method with existing techniques

Author- (Year)	Scheme	Method Novelty & Advantages	Drawbacks	Complexity
Mohamad .et.al.-2017 [10]	Cluster based	- The technique is effective since it only makes use of symmetric encryption - It offers defence against attacks using stolen smart cards, privileged insider attacks, and impersonation	Storage over head is more as Gate way needs to store three parameters for a single node.	$O(\log N)$

Priyanka Ahlwat et al. 2018 [4]	Matrix based	Resilience against node capture.	Need to optimize the values of factors used for relation of direct to indirect compromise.	$O(N^3)$
Quazi Mamun et al. 2019[37]	Cluster based	Less computational overhead in cluster formation phase and authentication phase.	Number of partial keys stored in memory is huge, which concerns reliability and security of the algorithm.	$O(\log N)$
Yinzi Tu et al. 2019[11]	Hash based	Key update process is completely controlled by the user it does not depend on Identity Generation Center (IGC)..	Memory overhead for key node a sit needs to store all the data backup.	$O(mN)$
Chien-Lung Hsu et al. 2020[14]	Group key based	It is resistant to impersonation, replay, and password guessing attacks. It offers the distribution of dynamic group keys. supports a multi-server setting.	Required number of parameters for authentication is high.	$O(N^3)$
Dashmetkaur Ajmaniet al. 2020[16]	Group key based	This scheme handles keys for multiple groups in the same Destination Oriented Directed Acyclic Graph (DODAG) Node.	Process of initialization and regeneration is comparatively slow.	$O(N^3 \log^3 Q)$
A.Singh et al. 2021[10]	Matrix based	This scheme deals with dynamism in Key agreement.	Packet delay is increasing over the number of nodes	$O(N^3)$
Padma shree M Getal. 2021[38]	Group key based	Reduced time complexity of there-keying operation by using cluster head of chosen IoT Devices. It performs better than Distributed Group Key Management	It utilizes more computation time than DGKM while the key is reset after device unsubscribes.	$O(\log N)$
Ksowjanya et al. 2021[28]	Public key based (ECC)	The scheme is key-escrow free and provides resistance against collusion attack. Size of the public key is significantly less as compared to other schemes.	The scheme does not provide security against physical capture attack and DoS attack.	$O(\log N)$
Cong Wang et al. 2022 [20]	ECC-based key agreement scheme	An ECC-based key agreement system is suggested for use with mutual anonymous authentication to secure communications.	Does not provide integrity through the scheme. Did not provide security analysis.	$O(N^3)$
Xing Su et al. 2023 [53]	Publicly based ECC scheme	Lightweight certificate-based authentication method based on the elliptic curve digital signature algorithm and cryptographic hashing.	The scheme does not provide security against physical capture attacks.	$O(N)$
Our method	ECC and hash based authenticated key agreement	An efficient ECC-based key agreement system for lightweight environment (IoT)	No drawbacks.	$O(N)$

Table 1 offers a comprehensive comparison between our method and existing key management techniques in the realm of IoT.

3. PROPOSED AUTHENTICATED KEY AGREEMENT SCHEME FOR IOT

This paper presents a proposal for implementing an authenticated group key management system in an Internet of Things (IoT) context. The establishment and dissemination of a shared secret value among network sensor nodes is a crucial objective in the field of computing. The key in question, referred to as either a group key or conference key (CK), fulfils the function of encrypting and decrypting messages.

Proposed Algorithm: The IoT devices establish communication among themselves and with a gateway, which subsequently connects to a cloud server. However, Gateway must authenticate all of them before to initiating their conversation. Typically, it is quite simple to exploit these IoT devices in order to compromise their security and expose their privacy on the network due to their public accessibility and constrained resources.

Our proposed authenticated key management protocol contains 4 phases:

- 1) User Registration phase
- 2) Authentication phase
- 3) Key Agreement

User Registration phase

- i. The smart device send device Id_i to the server (S).
- ii. Server uses Mk – message value, N_{id} -node Id , r_1 -random chosen value and calculates $H_1(Mk \parallel NID \parallel r_1)$
- iii. Server select its private key x_j $0 < j < n$, and calculate $N_s = H_1(Mk \parallel N_{ID} \parallel r_1) \oplus x_j$ for smart device.
- iv. The server subsequently computes the curve point N_s' by multiplying N_s with G and shares it with the devices.
- v. The server assigns a random number, nd , to each device, D_i . and server calculates $B_i = H(R_i \oplus H(X_s).N_s)$ and store calculates $B_i' = B_i .G$ and ID_i in the database.
- vi. In addition, server S transfers N_s' to the device D_i . Then D_i receives N_s' and it stores in the memory.

Login and Authentication

- i. In this phase the IoT device D_i generates a random nonce n_1 , calculates P_1 and P_2 and sends N_1 , P_1 and P_2 .
 $P_1 = n_1 \times G$, $P_2 = H(P_1 \parallel n_1 \times N_s')$
- ii. S recollects the associated record of the i^{th} device ID_i from the memory and computes the N_s value using Mk , N_{ID} and r_1 , then verifies the validity of P_2 .
- iii. If P_2 validation holds, then server(S) randomly generates the number N_2 , calculates P_3 and P_4 and send them to D_i , $P_3 = N_2 \times G$
Compute $P_4 = H(P_2 \parallel N_2 \times B_i')$
- iv. After obtaining the messages from server, the device(D_i), and computes $B_i = H(N_{ID} \parallel N_s')$

Key agreement

- i. Then device (D_i) verifies the correctness of P_4 and if it is verified successfully, it calculates V_i and SK . Then V_i is sent to server for the authentication and session key SK_i computed and agreed upon during this session.
 - i. $V_i = H(P_4 \parallel N_1 \times P_3)$
 - ii. $SK_i = H(P_3 \parallel N_1 \times P_3)$

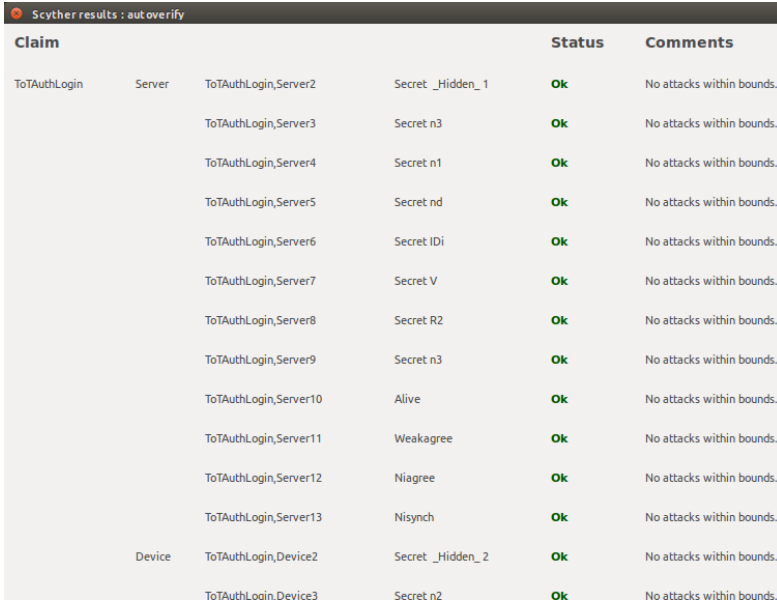
- ii. The server S checks the received V_i with computed V' and if both are same then, it computes session key SKs for the secure communication. Otherwise, the session is terminated.
- iii. Session key is $SK_s = H(P3 || N2 \times P1)$.

4. SECURITY ANALYSIS

This section explains an in-depth security analysis of the authentication and key exchange technique utilizing the Scyther tool. Scyther is a software tool that utilizes formal verification techniques to examine security protocols. This tool enables the precise definition and validation of cryptographic protocols, including authentication methods.

ScytherIoTAuthMain - Proto Description
<pre> macro V1 = H(ScalarMultiply(n3,Rd)); macro SK = H(ScalarMultiply(ScalarMultiply(R2,n3),Rd)); send_6(Server,Device,V1,R5); claim(e1,e2); claim(e1,e3); claim(e2,e5); claim(e3,e6,e7); } role Device { fresh ri,nd,n2 : Random; var n1,n3:Random; #var Rd,R1s, R5,V1:Nonce; macro IDi = ScalarMultiply(ri,Di); send_1(Device,Server,{IDi}k(Server,Device)); recv_2(Server,Device,{nd}sk,Rd); recv_3(Server,Device,R1s); macro R2 = ScalarMultiply(n2,G); macro R3 = ScalarMultiply(n2,R1s); macro R4 = ScalarMultiply(n2,Rd); macro V = H(ScalarAddition(R3,R4)); send_4(Device,Server,R2); send_5(Device,Server,V); recv_6(Server,Device,V1,R5); macro V1d = H(ScalarMultiply(nd,R5)); match(V1d,V1); macro SK1 = H(ScalarMultiply(ScalarMultiply(R2,n3),Rd)); claim(e4,Alive); claim(e4,Nisynch); claim(e4,Niagree); claim(e4,Secret,nd); } } e1 = Server, e2=Alive, e3=Nisynch, e4=Device, e5=Niagree, e6=Secret,e7=nd, </pre>

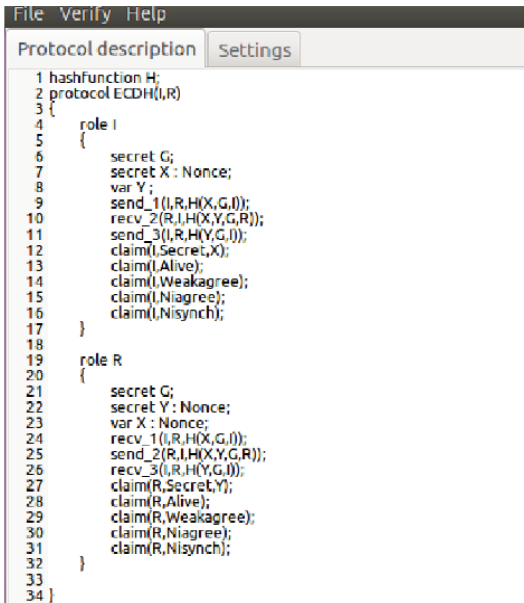
Fig 4: Scyther Code for Authentication



Claim	Status	Comments
ToAuthLogin Server ToAuthLogin_Server2 Secret _Hidden_ 1	Ok	No attacks within bounds.
ToAuthLogin_Server3 Secret n3	Ok	No attacks within bounds.
ToAuthLogin_Server4 Secret n1	Ok	No attacks within bounds.
ToAuthLogin_Server5 Secret nd	Ok	No attacks within bounds.
ToAuthLogin_Server6 Secret IDi	Ok	No attacks within bounds.
ToAuthLogin_Server7 Secret V	Ok	No attacks within bounds.
ToAuthLogin_Server8 Secret R2	Ok	No attacks within bounds.
ToAuthLogin_Server9 Secret n3	Ok	No attacks within bounds.
ToAuthLogin_Server10 Alive	Ok	No attacks within bounds.
ToAuthLogin_Server11 Weakagree	Ok	No attacks within bounds.
ToAuthLogin_Server12 Niagree	Ok	No attacks within bounds.
ToAuthLogin_Server13 Nisynch	Ok	No attacks within bounds.
Device ToAuthLogin_Device2 Secret _Hidden_ 2	Ok	No attacks within bounds.
ToAuthLogin_Device3 Secret n2	Ok	No attacks within bounds.

Fig 5: Scyther Verification for Authentication

Figures 6 and 7 depict the protocol through the use of a formal modeling language. They clearly outline the responsibilities of participants, provide detailed information about the messages sent, and explain the security properties required for validation. Afterwards, the program does an automatic analysis to assess the protocol for possible security weaknesses, such as authentication failures, replay attacks, or key leaks.



```
File Verify Help
Protocol description Settings
1 hashfunction H;
2 protocol ECDH(I,R)
3 {
4   role I
5   {
6     secret G;
7     secret X : Nonce;
8     var Y;
9     send_1(I,R,H(X,G,I));
10    recv_2(R,I,H(X,Y,G,R));
11    send_3(I,R,H(Y,G,I));
12    claim(L,Secret,X);
13    claim(L,Alive);
14    claim(L,Weakagree);
15    claim(L,Niagree);
16    claim(L,Nisynch);
17  }
18
19  role R
20  {
21    secret G;
22    secret Y : Nonce;
23    var X : Nonce;
24    recv_1(I,R,H(X,G,I));
25    send_2(R,I,H(X,Y,G,R));
26    recv_3(I,R,H(Y,G,I));
27    claim(R,Secret,Y);
28    claim(R,Alive);
29    claim(R,Weakagree);
30    claim(R,Niagree);
31    claim(R,Nisynch);
32  }
33 }
34 }
```

Fig 6. Scyther Code for Key agreement

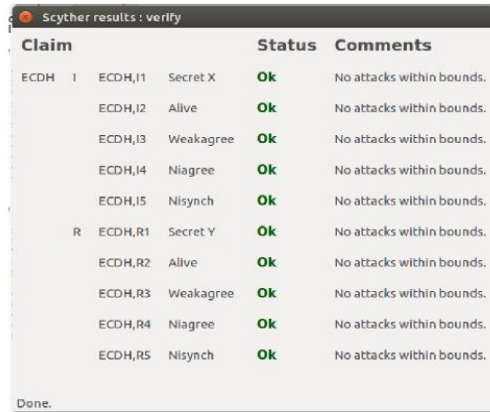


Fig 7: Scyther Verification for Key agreement

The investigation conclusively shows that our proposed authentication and key agreement techniques exhibit robust resistance against standard cyber assaults. These techniques have been rigorously tested and proven effective in safeguarding sensitive data and maintaining the integrity of communication channels within IoT networks.

Comparative analysis with exiting schemes

When evaluating our methodology in comparison to existing key management strategies in IoT, it is crucial to consider various threats specified in Table 5.1, which encompass the following: The following attacks are: P1-Man-in-the-Middle (P1-MIM) assault, P2-Replay attack, P3-Impersonation attack, P4-Message Integrity attack, and P5-Traceability attack. Each attack poses distinct challenges and threats to the security of IoT systems.

Table 2: Proposed method vs other existing methods

Method (Ref.)	Techniques used	P ₁	P ₂	P ₃	P ₄	P ₅
[41]	Elliptic Curve Crypto	No	Yes	No	No	No
[49]	Elliptic Curve Crypto& Hash function	No	No	Yes	No	No
[36]	Elliptic Curve Crypto& Hash function	Yes	Yes	No	Yes	No
[5]	Elliptic Curve Crypto& Hash function	No	Yes	No	Yes	No
[18]	Elliptic Curve Crypto& Hash function	No	Yes	Yes	Yes	No
[23]	Elliptic Curve Crypto& Hash function	Yes	No	No	No	Yes
Our method	Elliptic Curve Crypto& Hash function	Yes	Yes	Yes	Yes	Yes

Our solution improves the security of IoT systems by effectively tackling these assaults. It reduces potential vulnerabilities and guarantees the integrity, secrecy, and authenticity of communication channels.

Research Directions

In this section, we present importance and security enhancements that are required for future communication technologies.

Authentication and Key Agreement

The majority of the devices in IoT networks consist of sensors and actuators that are responsible for gathering sensitive data, highlighting the importance of heightened privacy and security [21,40]. A small number of message exchanges should make up the authentication mechanism, and verification should require little computational effort. Then it will be appropriate for an IoT ecosystem with devices that have limited resources. Because of its connection to the internet, the IoT network experiences a disproportionately higher number of attacks. Replay, DoS, impersonation, and man-in-the-middle (MIM) assaults are the most frequent forms of attacks. These networks must have an effective defence security plan.

Since the system is highly adaptable and effective for making simple database interactions, two factor and multi factor authentication methods are employed to ensure the authorisation of the proper user. Every one of these requirements must be met. Most IoT devices are constrained devices with low processing power [10,28]. It is no longer appropriate to use conventional authentication techniques. Data transfer can be protected, however overall data security cannot be ensured. By creating new, simpler algorithms, the existing solutions to security, privacy, and authentication problems in a range of settings, such as mobile, cloud, and internet computers, can be improved.

5. CONCLUSION AND FUTURE WORK

Authentication and key management are the processes used to address the issues with key identification, setup, distribution, periodic renewal, and maintenance [9,21,22]. The security and defence of any network must include authentication and key management. Being concerned only with primitives that fulfil a certain security goal is insufficient in the IoT space. The IoT key management, authentication, and trust management scheme that was initially suggested in this study is described along with its methodology, advantages, and disadvantages. This work proposes an authenticated key management protocol utilizing a symmetric key technique to tackle the aforementioned challenges. Our technique has undergone rigorous testing with security analysis tools such as Scythur, demonstrating its resilience against known attacks. Additionally, the benefits, drawbacks, and unresolved problems are covered, as well as potential new directions for the finest security solutions.

Future IoT security will be a dynamic field, with new breakthroughs and difficulties appearing as the number of connected devices rises [35,38]. The improvement of IoT security as a whole will probably continue to receive attention in the years to come, including efforts to address flaws in the devices themselves, the communication networks they use, and the cloud and data centers where their data is kept. This could include enhancing encryption and authentication techniques, introducing new security protocols and standards, and protecting IoT networks and devices. Additionally, there will be a stronger focus on creating technologies and tools to identify and address security incidents and threats, as well as strengthening the resistance of IoT systems to cyberattacks. Ensuring secure communication between sensors and servers is a significant challenge in IoT systems [4,8]. The focus of our upcoming research is to develop a very efficient and secure method for managing authentication keys in IoT networks that are integrated with cloud services. The following are some unresolved challenges [14,18,22] for the proposal of an effective lightweight authenticated key management: The key management system has some limitations, including the cost of creating and distributing keys after a delay and potential communication delays. Given the small size, limited energy, restricted capabilities, and limited resources of sensors, it is imperative to have a security solution that is lightweight. It is capable of fulfilling trust and key management needs. Nodes can be added or withdrawn in any network sometimes. The newly added node and the previously eliminated node both endanger the network. Therefore, the creation of a secure mechanism for adding new nodes and updating keys after node removal is necessary for a secure network. In low-resource settings, public key cryptography was expensive and sluggish. Speed is important because it enables sensor nodes to practically establish a secure connection in a matter of seconds. Creating an easy-to-use, anonymous user authentication mechanism to establish a secure connection between the gateway and sensor nodes in IoT-based applications.

References

1. H. Chan, A. Perrig, and D. Song (2003) Random key pre-distribution schemes for sensor networks, "In Proceeding of Security and Privacy Symposium, pp. 197-213 23.
2. Gandino F, Montrucchio B, Rebaudengo M (2009) Key management for static wireless sensor networks with node adding. *IEEE Trans Ind Inform* 10(2):1133–1143.
3. Chen, S. Y., Song, S. F., Li, L. X., & Shen, J. (2009). Survey on smart grid technology. *Power System Technology*, 8, 1-7.
4. J. Zhang and V. Varadarajan, "Wireless sensor network key management survey and taxonomy," *J. Netw. Comput. Appl.*, vol. 33, no. 2, pp. 63–75, 2010.
5. L. Ham and C. Lin, "Authenticated group key transfer protocol based on secret sharing," *IEEE Trans. Comput.*, vol. 59, no. 6, pp. 842–846, Jun. 2010.
6. J.-H. Son, J.-S. Lee, and S.-W. Seo, "Topological key hierarchy for energy-efficient group key management in wireless sensor networks," *Wireless Pers. Commun.*, vol. 52, no. 2, pp. 359–382, 2010.
7. C.-Y. Lee, Z.-H. Wang, L. Harn, and C.-C. Chang, "Secure key transfer protocol based on secret sharing for group communications," *IEICE Trans. Inf. Syst.*, vol. 94, no. 11, pp. 2069–2076, 2011.
8. J. Liu, Y. Xiao and C.L. Philip Chen, Authentication and Access Control in the Internet of Things, ICDCSW, 2012, 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops 2012, pp. 588-592.
9. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013b). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.
10. P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications," *Int.J. Distrib. Sensor Netw.*, vol. 2014, Jul. 2014, Art. ID 357430.
11. Yosra BenSaïeda, Alexis Olivereau, Djamel Zeghlache, Maryline Laurent, Lightweight collaborative key establishment scheme for the Internet of Things, *Computer Networks*, Volume 64, 2014, pp. 273-295.
12. X. Fan and G. Gong (2015) LPKM: A lightweight polynomial-based key management protocol for distributed wireless sensor networks," In proceeding of International Conference on Ad Hoc Networks, pp. 180-195.
13. Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., Tenhunen, H. (2015). SEA: secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Computer Science*, 52, 452-459.
14. S. Sciancalepore, A. Capossele, G. Piro, G. Boggia and G. Bianchi, Key Management Protocol with Implicit Certificates for IoT systems, *IoT-Sys 15 Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*, 2015, pp. 37-42.
15. A.N.Tentu, Dileep Kumar P, V.Ch. Venkaiah, Allam Apparao, Sequential Secret Sharing for Level Ordered Access Structure, *Journal of Network Security*, Vol.18, No.5, PP.874-881, 2016
16. Z. Drias, A. Serhrouchni and O. Vogel (2017), "Identity-based cryptography (IBC) based key management system (KMS) for industrial control systems(ICS)," 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, pp. 1-10, doi: 10.1109/CSNET.2017.8242008.
17. Shin, D., Sharma, V., Kim, J., Kwon, S., & You, I. (2017). Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks. *IEEE Access : Practical Innovations, Open Solutions*, 5, 11100-11117.
18. A.N.Tentu, Abdul Basit, K. Bhavani, V. Ch. Venkaiah: Sequential (t,n) multi secret sharing scheme for level-ordered access structure, *Journal of Information Technology*, Vol10, pp 111, 2018, Springer.
19. S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for BLE-based devices in the internet of things," *IEEE Access*, vol. 6, pp. 24 639–724 649, 2018.
20. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Comput. Secur.* 2018, 78, 126–142.
21. Ko, I. Y., Ko, H. G., Molina, A. J., & Kwon, J. H. (2016). SoIoT: Toward a user-centric IoT-based service framework. *ACM Transactions on Internet Technology (TOIT)*, 16(2), 1-21.
22. Zhang, M., Wang, C., Wang, J., Tian, S., & Li, Y. (2018). A new approach to security analysis of smart home authentication systems. *Fundamental Informatica*, 157(1-2), 153-165.
23. Pramod T. C., Thejas G. S., S. S. Iyengar, N. R. Sunitha (2019), CKMI: Comprehensive Key Management Infrastructure Design for Industrial Automation and Control Systems, *Future Internet*, vol-11, issue-126.
24. Hao, J.; Liu, J.; Wang, H.; Liu, L.; Xian, M.; Shen, X. Efficient Attribute-Based Access Control With Authorized Search in Cloud Storage. *IEEE Access Security. Priv. Cloud IoT* 2019, 7, 182772–182783

25. M. K. B, M. S. Kumar, F. D. Shadrach, S. R. Polamuri, P. R and V. N. Pudi, "A binary Bird Swarm Optimization technique for cloud computing task scheduling and load balancing," 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2022, pp. 1-6, doi: 10.1109/ICSES55317.2022.9914085.
26. Ding, S.; Cao, J.; Li, C.; Fan, K.; Li, H. A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. *IEEE Access Secur. Priv. Cloud IoT* 2019, 7, 38431–38441.
27. Avanija, J., K. E. Kumar, Ch Usha Kumari, G. Naga Jyothi, K. Srujan Raju, and K. Reddy Madhavi. "Enhancing Network Forensic and Deep Learning Mechanism for Internet of Things Networks." (2023).
28. Khalid, U.; Asim, M.; Baker, T.; Hung, P.C.; Tariq, M.A.; Rafferty, L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Clust. Comput.* 2020, 23, 2067–2087.
29. A.N.Tentu, Kallepu Raju, V. Ch. Venkaiah, Cryptanalysis of a Group Key Transfer Protocol: Generalization and Countermeasures, *Journal of Combinatorics, Information & System Sciences (JCISS): A Quarterly International Scientific Journal*, Vol.44, 2020.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

