https://africanjournalofbiomedicalresearch.com/index.php/AJBR
Afr. J. Biomed. Res. Vol. 27 (September 2024); 142-149

Research Article

Efficient Lightweight Authenticated Key Management Protocol for Iot-Based Environment

N Subbareddy Ramireddy[1], Kolla Bhanu Prakash[2*]

*[1,2]*Dept. of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur District, A.P., INDIA*

ABSTRACT

The Internet of Things (IoT) is a network of interconnected objects that communicate by transmitting and receiving data. The assurance of data confidentiality while transmission across an unsecured network is contingent upon effective key management. Acquiring a authenticated key management strategy is challenging due to the high energy and computational expenses, despite the existence of several feasible key management strategies. In order to address this problem, various key management protocols have been proposed. These protocols aim to resolve the issue of having a single point of failure and ensure the security attributes of the current system are maintained.

In this paper, we propose a novel light weight key management mechanism for wireless sensor networks and its integration into the Internet of Things. A technique that requires authentication is implemented using elliptic curve and hash algorithms and presented efficient key agreement scheme for establishing session key. This method also offers the functionality of adding and removing clients, as well as ensuring the freshness of encryption keys. Experimental results and security analysis of proposed method is presented. Our scheme is an efficient and compared results with existing techniques.

Keywords: Internet of Things, Protocol, Elliptic curve, Hash algorithms, Encryption

**Author for correspondence: Email: drkbp@kluniversity.in*

Receiving Date: 10/07/2024 Acceptance Date: 20/08/2024

DOI: https://doi.org/10.53555/AJBR.v27i3.1948

INTRODUCTION

Cryptographic key management is the process that addresses the issue of generating, establishing, distributing, and maintaining confidential session keys. This chapter specifically examines group communication that incorporates confidentiality measures to restrict access to material shared inside a secure communication session to only authorized group members. Ensuring the secrecy of information in wireless sensor networks (WSNs) involves the crucial duty of establishing and maintaining a shared session key among group members. Wireless sensor networks play a crucial role in the development of IoT technology [14]. The installation of a group key is crucial for ensuring the integrity, authentication, and confidentiality of message transmissions within multicast groups. In addition, group key establishment procedures in IoT-enabled WSNs must be able to accommodate the specific characteristics of devices and networks, including resource limitations, scalability, and the ability to build dynamic groups. Wireless sensor networks [15] are comprised of numerous nodes that self-organize without central supervision. Nodes that are beyond the transmission range can connect using multi-hop routing. The Internet of Things (IoT) has emerged as a potent component of advanced networking technologies. In an ecosystem enabled by the Internet of Things (IoT), tangible objects or things are no longer unresponsive. Instead, they possess connectivity to the Internet and are equipped with processing and communication capabilities.

Security in IoTs devices

The Internet of Things (IoT) and the 5G communication environment allow various applications, including remote surgery, self-driving automobiles, virtual reality, flying IoT drones, security and surveillance, among others [3,4,5]. In addition, it is vulnerable to numerous possible threats such as replay attacks, impersonation, password guessing, physical device theft, session key calculation, privileged insider attacks, malware, man-in-the-middle attacks, malicious routing, and others. Hence, it is imperative to safeguard the infrastructure of the 5G-enabled IoT communication environment from such attacks. To tackle this issue, researchers in this domain need to develop a range of security protocols categorized into key management, user authentication/device authentication, access control/user access control, and intrusion detection. A fundamental cryptographic primitive known as key management serves as the foundation for all other security primitives. Key management is divided into pairwise and group key management systems depending on the application.

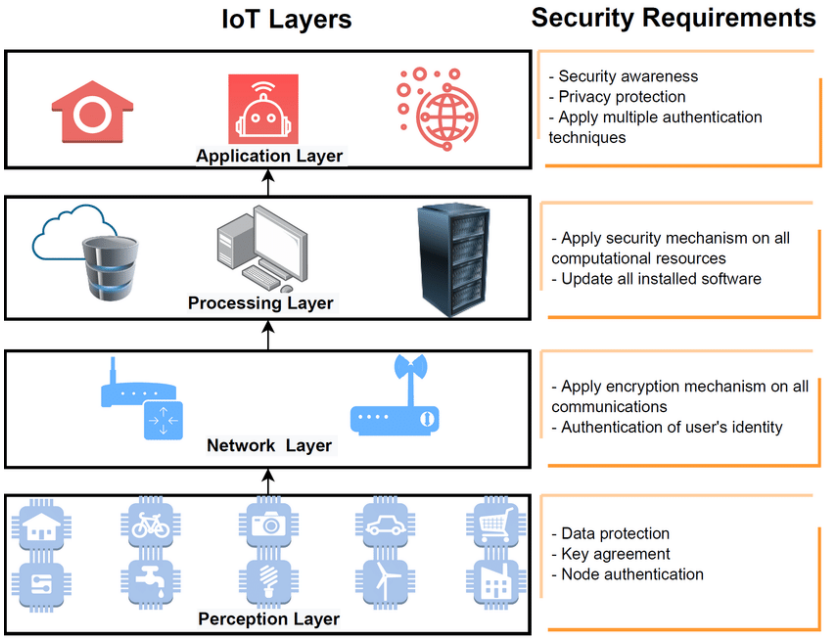


Fig 1: IoT: Security Requirements

Figure 1 presents detailed layer wise security requirements in which authentication and key agreement play a very important role in perception layer to application layer. Locally broadcast communications are typically secured using Group keys, which are shared keys [6,7] across all group members. The base station uses a group key, which is a globally distributed common key, to encrypt communications that are broadcast to the whole network. Key management in wireless sensor networks (WSNs) and other communication protocols is difficult in terms of applicability. In WSNs, public key cryptography or symmetric cryptography algorithms were the basic building blocks of key management techniques.

In homogeneous sensor networks, the majority of key management strategies focus primarily on employing symmetric cryptosystems, although they frequently have poor storage performance and have a high overhead when creating shared keys for all neighboring sensor pairs. An early study [7,8, 24] used blockchain as a distributed service platform for IoT to confirm the viability of blockchain-based IoT applications. Its performance analysis clearly shows that distributed fog-node performance is significantly superior to that of a centralized cloud, which we can adopt for our proposed method. We incorporate the benefits and features of blockchain technology into IoT communication and provide an effective blockchain-based verified group key agreement protocol for IoT applications. The majority of today's resource-constrained IoT devices, however, are not yet able to interface directly with a blockchain.

Motivation and Contribution

The majority of security mechanisms [2,13] offered for the IoT environment are inadequate as they fail to provide comprehensive protection against potential assaults. In addition, several protocols are effective against specific attacks but are ineffective against multiple simultaneous attempts. Therefore, it is imperative to develop security mechanisms that can simultaneously safeguard against numerous threats. Hence, the development of protocols for this specific domain is a formidable challenge that must be addressed by future scholars. Security is of utmost importance in nearly all IoT applications [14,15] that have been implemented or are currently being implemented. The utilization of IoT is expanding at a quick pace and infiltrating a majority of the current sectors. While operators do provide support for IoT applications using current networking technologies, many applications require stronger security measures from the technology they rely on.

Our Contribution

This paper presents, an efficient method for user authentication and key agreement that is both lightweight and anonymous is a crucial undertaking in IoT-based systems [16], ensuring secure connection between the gateway and sensor nodes.

i. We propose a new and efficient authenticated key management technique for wireless sensor networks, which is also seamlessly integrated into the Internet of Things.
ii. An authentication technique is constructed utilizing elliptic curve and hash algorithms to establish a session key through an efficient key agreement scheme.
iii. This method additionally provides the capability to add and remove customers, while also maintaining the up-to-date nature of encryption keys.
iv. We experimented propose scheme and presented a thorough security analysis of the proposed approach.

Organization of the Paper

The rest of the paper is organized as follows: In section 2, we present authentication key agreement schemes and section 3 explains the related work and the drawbacks in existing methods. Section 4 discusses the proposed method procedure and its overview and experiment results presented in section 5. Security analysis of the proposed method is presented in section 6, section 7 concludes the paper and future work.

AUTHENTICATION AND KEY MANAGEMENT PROTOCOLS

This section presents various authentication and key management systems that are suited for IoT environment.

Authentication and Key Agreement

Using different passwords at every step of authentication could be a tedious task for the user, hence several other techniques for the same are taken in use like the fingerprint scan, iris scan etc. Also, considering only one factor for authentication was not sufficient as it has risks for hacking and loss of personal data. To guarantee the correct user is authorized, two factor and multi factor authentication methods are employed. The system is highly adaptable and efficient, facilitating seamless interactions with the database. There are several already existing researches in this particular sector but there's always a scope of improvement and adding additional security to it. An authentication technique that is secure can ensure both secure connections and secure data. Implementing authentication techniques [25,31] for IoT devices is a difficult task. Authentication encompasses three crucial elements: security, which guarantees the confidentiality of the user's long-term secret across all locations and at all times; storage efficiency. Information presented by one party to another to authenticate itself, it can use hash, symmetric or asymmetric cryptographic algorithms.

Taxonomy of IoT Authenticated Key Management Schemes

We present most recent literature on key management schemes in IoT environment.

i. Asymmetric key management schemes

Public Key Cryptography [42,43] in server nodes necessitates robust computational nodes and dedicated cryptographic processors. For client nodes that have applications requiring occasional connections to other servers, Public Key Cryptography (PKC) could be a suitable option. Pre-shared key methods are beneficial for server nodes in compact real-world applications. Nevertheless, currently available mathematical-based Key Management Systems (KMS), such as the Polynomial scheme, offer superior characteristics provided that the application can handle the additional computational burden. Note that such Key Management Systems (KMS) can also function as a feasible solution for client nodes. The methodology presented in references [16,44] provides techniques to guarantee confidentiality and end-to-end guarantees by employing group-based keys within a clustered and distributed key management system. A Denial of Service (DoS) attack can be executed in the provided manner, as it fails to impose any restrictions on users, allowing them to send superfluous messages to the cluster head. The scheme has a computational complexity of $O(N^3)$.

ii. Group Key Management in constrained IoT Settings

In [39,40] presented a systematic summary of GKM protocols, taking into account various key distribution models as categorization criteria. The analysis of synchronous and asynchronous GKM methods reveals that current approaches either lack reliability mechanisms or provide mechanisms that are ill-suited for the specific dynamically evolving limited environment. Centralized synchronous protocols have methods that are appropriate, but they are not scalable for the specific dynamically-changing circumstances they are designed for. Constrained environments lack reliability when using any asynchronous protocols. Reliability mechanisms are currently absent in lightweight centralized asynchronous protocols. In the paper [22], presents a highly scalable multi-group key management protocol for IoT that ensures forward and backward secrecy, effectively recovers from the collision attack and provides secure coexistence of several services.

iii. Public key authentication and key agreement

The techniques [38] overcomes the substantial airtime usage necessary for exchanging messages for authentication and key agreement. The solution offers a unique key management protocol that combines implicit certificates with a typical elliptic curve Diffie-Hellman exchange. It facilitates authentication and key agreement. The system offers the ability to derive temporary keys, perform rapid key updates, and effectively defend against replay assaults. The results demonstrate a reduction in airtime usage of up to 86.7% compared to traditional methods that rely on X.509 certificates. The method lacks protection against node capture attacks or impersonation attacks, and it does not optimize the utilization of memory and computing power. The scheme has a computational complexity of O(log N).

iv. Matrix based key management schemes

The study in [35,36,37] examines the issue of node capture attack from an adversarial perspective, where the opponent strategically exploits the weaknesses. In order to counteract, the strategy creates an analogous assault matrix. This matrix delineates a group of pivotal nodes and provides them a hierarchical dominance ranking. It is necessary to optimize the values of components that contribute to direct and indirect compromise. The scheme has a computational complexity of $O(N^3)$. A matrix-based approach for key management was introduced in [34,38], which utilized encryption techniques to optimize storage capacity and reduce the computational burden on nodes. This plan Enhances the robustness of node capture.

Additionally, it provides enhanced storage capacity. The client experiences a higher level of communication overhead when disconnected as a result of network failure. The computational complexity of the scheme is expressed as O(m∗N).

RELATED WORK

With 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 fairly reliable 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 protocols [1,2,3] is its guarantee of the integrity and validity of message transactions.

In [4] 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. [6] 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 in [2]. 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 [14]. 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 [15], 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, [16] offers a solution and techniques for achieving confidentiality and end-to-end guarantees. It uses a clustering strategy to spread the massive IoT network.

In [18], a matrix-based approach to key management was developed. To increase store capacity and make nodes lighter, the approach leveraged encryption. With this technique, node capture resilience is improved. Additionally, it offers more storage room. In the event of a network outage, the client experiences increased communication overhead. A lightweight authentication and key agreement approach for WSN in an IIOT environment is suggested in [19]. Fast authentication and an unpredictably long pseudonym update period were the outcomes of the suggested effort. A logical tree-based secure mobility management method (LT-SMM) leveraging mobile service computing has been suggested in [21]. To guarantee message integrity, it has used chaotic map-based one-way hash algorithms. It reduces and fixes concerns with additional rekeying. The study [22] introduces a highly scalable multi-group key management protocol for the Internet of Things that guarantees forward and backward secrecy, successfully fends off collision attacks, and permits the coexistence of different services in a secure manner.

A mutual authentication and session key agreement technique is suggested in [25] article to ensure safe communication in IoT-enabled WSNs. To create a session key, Weil pairing and ECC are used. As the receiver recognizes the replayed message by checking the nonce, the Scheme is protected from replay attacks.

PROPOSEDLIGHTWEIGHT AUTHENTICATED KEY AGREEMENT SCHEME

In this section, our focus is on authenticated group key management for IoT environment. 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. Firstly, we present important cryptographic techniques for construction of our methods.

Elliptic Curve Cryptography

In order to execute an already established system, we require an elliptic curve [7,8]. A function E defined over a finite field F can be expressed as $y2 = x3 + ax + b$, where a and b are members of the finite field F with pn elements, where p is a large prime number. The equation is satisfied by the set of points (x,y) that belong to the set F. In geometric terms, the addition of two points (Q1) and (Q2) involves drawing a straight line that intersects both points and finding the third intersection with the curve (R1). Reflecting this point (R1) along the x-axis results in the sum of (Q1) and (Q2), denoted as (Q1) + (Q2).

Hash function

A hash function H(M) [5,6] generates a hash h of a fixed length from a message of variable length. The length of the hash h remains constant regardless of the length of the message M, even if it is as large as a terabyte. The hash value h, which possesses the attribute of being one-way, cannot be utilized to determine the message M. Reverse engineering is not feasible in this particular scenario. The equation h = H(M) defines it. For each distinct value of M, it generates a unique hash h. It aids in detecting any alterations to the message M throughout its transit across the network. Modifying any part of the message M will result in a corresponding alteration in the hash value h = H(M) of the message. We can select SHA-1 with Block size 512, Word size 32 and with hash value 160, similary for other variants select SHA-256 with Block size 512, Word size 32 and with hash value 256, and SHA-512 with Block size 1024, Word size 64 and with hash value 612,

Proposed Authenticated Key Agreement Scheme

The IoT devices establish communication among themselves and with a gateway, which is then connected to a cloud server.

However, Gateway must authenticate each of them before to initiating their conversation. Typically, these IoT devices are vulnerable to attacks that compromise their security and expose their privacy on the network due to their public nature and limited resources. Our proposed authenticated key management protocol contains 3 phases:

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

User Registration phase

i. The smart device send device IDi to the server (S).
ii. Server uses Mk – message value, Nid-node Id, r1-random chosen value and calculates H1(Mk || NID || r1)
iii. Server select its private key xj 0<j<n, and calculate Ns = H1(Mk || N_{ID} || r1) ⊕ xj for smart device.
iv. The server then it calculates the curve point Ns' = Ns×G and shared with devices.
v. The server selects the random number nd for every device Di and server calculates B_i = H(Ri ⊕ H(Xs).Ns) and store calculates B_i' = B_i .G and IDi in the database.
vi. In addition, server S transfers Ns' to the device Di. Then Di receives Ns'and it stores in the memory.

Login and Authentication

i. In this phase the IoT device Di generates a random nonce n1, calculates P1 and P2 and sends N1, P1 and P2.

P1 = n1 × G, P2 = H(P1||n1 × Ns′)

ii. The S recollects the associated record of the ith device IDi from the memory and computes the Ns value using Mk, N_{ID} and ri, then verifies the validity of P2.
iii. If P2 validation holds, then server(S) randomly generates the number N2, calculates P3 and P4 and send them to Di , P3 = N2 × G

Compute P4 = H(P′2||N2 × B′i)

iv. After obtaining the messages from server, the device(Di), and computes Bi = H(N_{ID}||Ns′).

Key agreement

i. Then device (Di) verifies the the correctness of P4 and if it is verified successfully, it calculates Vi and SK. Then Vi is sent to server for the authentication and session key SKi computed and agreed upon during this session.

i. Vi = H(P′4 ||N1 × P3)
ii. SKi = H(P3||N1 × P3)

ii. The server S checks the received Vi 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 SKs = H(P3||N2 × P1).

The following algorithm explains the details of the interactive computations between server and device:

Algorithm 1: Authentication and Key agreement

Server **(*S*)**	Device (D_i)
1: D_i randomly generates n_2	
2: Compute $R_2 = n_2$ x G	
3: Compute $R_3 = n_2$ x R_1'	
4: Compute $R_4 = n_2$ x R_d	
5:Compute AuthenticationParameter $V=H(R_3+R_4)$	
6: Send $\langle V, R_2 \rangle$ to Server S	
7: Compute $V' = H(n_1 \times n_s \times R_2 + n_d \times R_2)$	
8: if V ==V' then	
9: Authentication Successful	
10: S randomly selects n_3	
11**:** Compute $R_5 = n_3 \times G$	
12: Compute $V_1 = H(n_3 \times R_d)$	
13: Compute $SK = H(R_2 + R_5 + R_d)$	
14: Send $\langle V_1, R_5 \rangle$ to D_i	
15**:** else	
16: Authentication Failed	
17: end if	
18: Compute $V_1' = H(n_d \text{ x } R_5)$	
19: if $V_1 == V_1'$ then	
20: Authentication Successful	
21: $SK' = H(R_2 + R_5 + R_d)$	22: else
23: Authentication Failed	
24: Endif	

EXPERIMENT RESUTLS

This section presents experiment results of our scheme in client and server platform. Implementation of proposed authenticated key agreement algorithm is done in two modules – IoT client-side module and Server-side node. The client-side code is implemented in Python that will be running on the Raspberry pi. The server-side code is implemented in JavaScript. A socket communication is established between both IoT node and server node.

Since the algorithm is ECC based, the selected curve for the implementation is –

Standard curve database

ANSI X9.63 curves, ansip256k1, 256-bit prime field Weierstrass curve.

Parameters:

p 0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffefffffc2f

a 0x0

b 0x7

G (0x79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798, 0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8)

n 0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141

h 0x1

Below snippets Fig 2 and Fig 3 shows the snapshot of login and authentication phase.

Fig 2 – Snapshot of Server-side Login and Authentication Phase

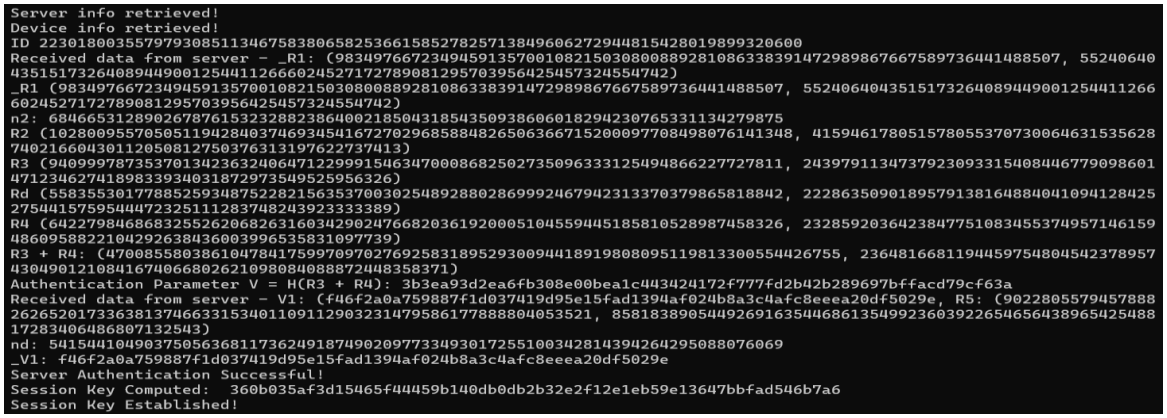


Fig 3 – Snapshot of Client-side Login and Authentication Phase

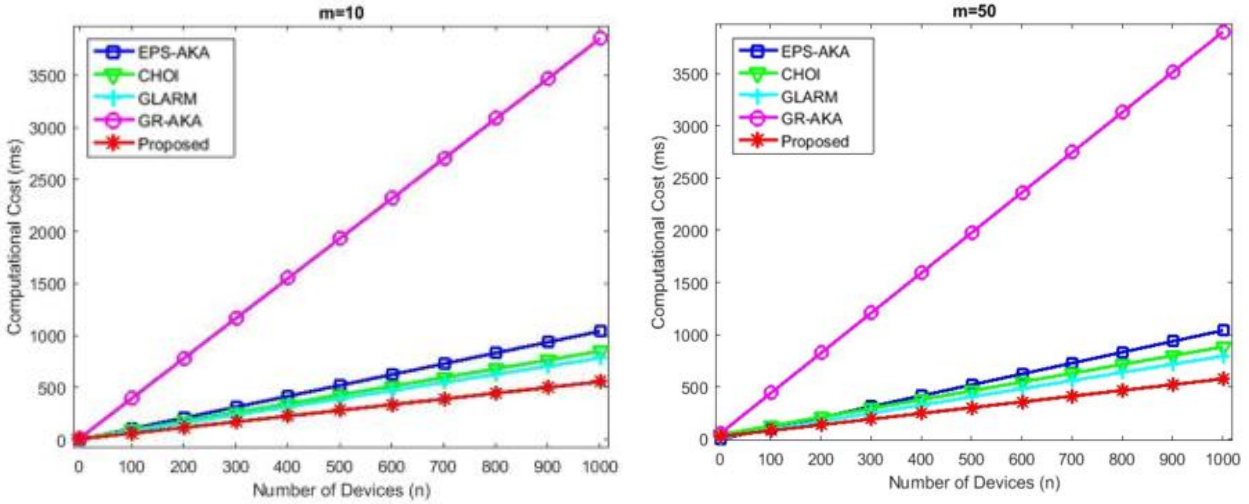
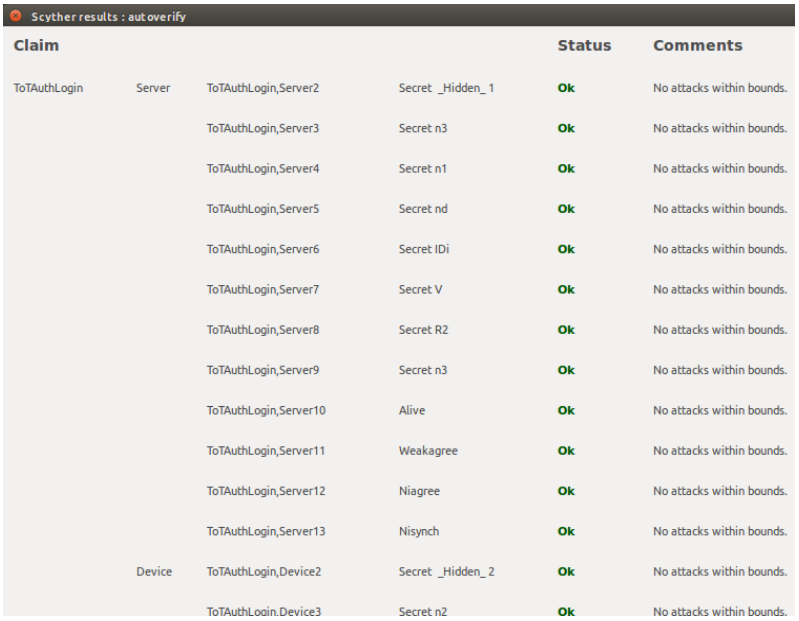


Fig. 4. Comparison of computational costs, for m = 10. **Fig.4**. Comparison of computational costs, for m = 50

Figures 4 and 5 illustrate the computing costs of the five investigated protocols as a function of the number of devices, specifically for certain values of m (where m represents the number of groups). The formulas and graphs demonstrate a direct relationship between the cost of communication and the number of devices (n), indicating that the cost increases in a linear manner. Under most conditions, the recommended protocol exhibits superior performance compared to current protocols when the number of devices is increased, provided that the number of groups is raised to 50.

SECURITY ANALYSIS

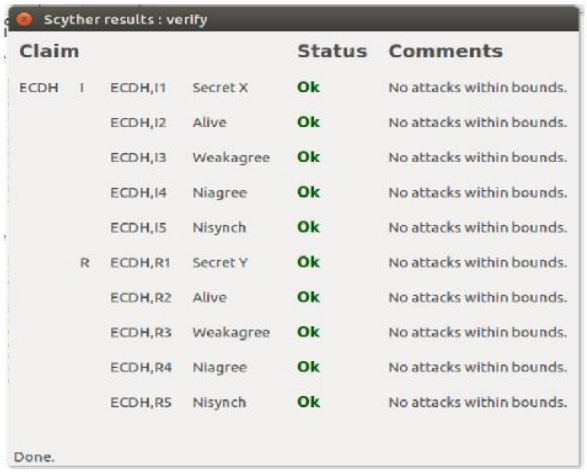
Security analysis tools, as defined by reference [21], are software programs or frameworks designed to facilitate the scrutiny and evaluation of the security of computer systems, networks, applications, or protocols. Scyther is an advanced tool designed for the analysis and validation of security systems.



Claim				Status	Comments
ToTAuthLogin	Server	ToTAuthLogin,Server2	Secret _Hidden_ 1	Ok	No attacks within bounds.
		ToTAuthLogin,Server3	Secret n3	Ok	No attacks within bounds.
		ToTAuthLogin,Server4	Secret n1	Ok	No attacks within bounds.
		ToTAuthLogin,Server5	Secret nd	Ok	No attacks within bounds.
		ToTAuthLogin,Server6	Secret IDi	Ok	No attacks within bounds.
		ToTAuthLogin,Server7	Secret V	Ok	No attacks within bounds.
		ToTAuthLogin,Server8	Secret R2	Ok	No attacks within bounds.
		ToTAuthLogin,Server9	Secret n3	Ok	No attacks within bounds.
		ToTAuthLogin,Server10	Alive	Ok	No attacks within bounds.
		ToTAuthLogin,Server11	Weakagree	Ok	No attacks within bounds.
		ToTAuthLogin,Server12	Niagree	Ok	No attacks within bounds.
		ToTAuthLogin,Server13	Nisynch	Ok	No attacks within bounds.
	Device	ToTAuthLogin,Device2	Secret _Hidden_ 2	Ok	No attacks within bounds.
		ToTAuthLogin,Device3	Secret n2	Ok	No attacks within bounds.

Fig 6: Scyther Verification for Authentication

Figures 6 and 7 depict the protocol using a formal modeling language, outlining the responsibilities of the participants, specifying the messages exchanged, and defining the security features to be validated. The program thereafter does an automated analysis to examine the protocol for possible security weaknesses, such as authentication failures, replay attacks, or key leakage.



Claim				Status	Comments
ECDH	I	ECDH,I1	Secret X	Ok	No attacks within bounds.
		ECDH,I2	Alive	Ok	No attacks within bounds.
		ECDH,I3	Weakagree	Ok	No attacks within bounds.
		ECDH,I4	Niagree	Ok	No attacks within bounds.
		ECDH,I5	Nisynch	Ok	No attacks within bounds.
	R	ECDH,R1	Secret Y	Ok	No attacks within bounds.
		ECDH,R2	Alive	Ok	No attacks within bounds.
		ECDH,R3	Weakagree	Ok	No attacks within bounds.
		ECDH,R4	Niagree	Ok	No attacks within bounds.
		ECDH,R5	Nisynch	Ok	No attacks within bounds.

Done.

Fig 7: Scyther Verification for Key agreement

The analysis proves our proposed authentication and key agreement protocols are resistant to standard attacks.

6.3 Comparative analysis with exiting schemes

We compare various techniques with our scheme and proposed method resistant to existing attacks.

Method	Techniques used	P_1	P_2	P_3	P_4	P_5
GPS-AKA [12]	ECC	X	✓	X	X	X
CHOI [14]	ECC+Hash	X	X	X	X	X
GLRAM[17]	ECC+Hash	✓	✓	X	✓	X
GR-AKA [32]	ECC+Hash	X	✓	X	✓	X
WCF [25]	ECC+Hash	X	✓	✓	✓	X
T.M.Butt[23]	ECC+Hash	✓	X	X	X	X
Our method	ECC+Hash	✓	✓	✓	✓	✓

Table 1. Our method vs other existing methods

The table 1 lists the following attacks: P1-MIM assault, P2-Replay attack, P3-Impersonation attack, P4-Message Integrity attack, and P5-Traceability attack. ✓ indicates resistance, while X indicates non-resistance.

CONCLUSIONS AND FUTURE WORK

Authentication and key management are vital elements of network security and safeguarding. When it comes to the IoT industry, it is not enough to only focus on basic elements that fulfill a specific security objective. This paper presents an efficient IoT authentication, key management, and trust management scheme for IoT environment. We implemented proposed scheme and performed security analysis. The purpose of this analysis is to evaluate security solutions and determine the one that most effectively meets the application's needs. Our method is efficient and resistant to existing attacks.

Future Work

Our plan is proposing an efficient framework for blockchain based lightweight authentication for IoT environment. By using a blockchain-based authentication system, this framework will provide a secure, decentralized, and tamper-proof method for managing IoT device identities and authorizations. In our framework, a distributed authentication system to verify and manage a network of Internet of Things (IoT) enabled devices, the system comprising: the multiple IoT enabled devices; a fog node connected to the each of the multiple IoT enabled devices, wherein the fog node: receives, a network registration request from an IoT enabled device that is selected from the IoT enabled devices.

REFERENCES

M.M. Modiri , J. Mohajeri 2 M. Salmasizadeh, A novel group-based secure lightweight authentication and key agreement protocol for machine-type communication, Volume 29, Issue 6 - Serial Number 6, Transactions on Computer Science & Engineering and Electrical Engineering (D), pp3273-3287, 2023.

Patruni Muralidhara Rao, B.D. Deebak, A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions, Ad Hoc Networks 146 (2023) 103159.

Mohammed Nafi, Mohamed-Lamine Messai, Samia Bouzefrane, Mawloud Omar, IFKMS: Inverse Function-based Key Management Scheme for IoT networks, Journal of Information Security and Applications Volume 71, December 2022, 103370.

Junfeng Miao, Zhaoshun Wang, Mei Wang, Xiao Feng, Nan Xiao, Xiaoxue Sun, Security Authentication Protocol for Massive Machine Type Communication in 5G Networks, Volume 2023 | Article ID 6086686.

Cong Wang, Su Li, Maode Ma, Xin Tong, Yiying Zhang, Bo Zhang, "A Noval and Efficient ECC-Based Authenticated Key Agreement Scheme for Smart Metering in the Smart Grid", Electronics, vol.11, no.20, pp.3398, 2022.

Xing Su, Yong Xie, Hongyuan Wang, Hui Wang, "Blockchain-based Privacy-preserving Authentication Key Agreement Protocol for Industrial Wireless Sensor Networks", 2022 IEEE 28th International Conference on Parallel and Distributed Systems (ICPADS), pp.234-241, 2023.

Thungon, L.C., Sahana, S.C. & Hussain, M.I. A lightweight certificate-based authentication scheme for 6LoWPAN-based internet of things. J Supercomput (2023).

Priyanka Mall, Ruhul Amin, Ashok Kumar Das, Mark T. Leung, Kim-Kwang Raymond Choo:PUF-Based Authentication and Key Agreement Protocols for IoT, WSNs, and Smart Grids: A Comprehensive Survey. IEEE Internet Things J. 9(11): 8205-8228 (2022)

Iqbal, U.; Tandon, A.; Gupta, S.; Yadav, A.R.; Neware, R.; Gelana, F.W. A Novel Secure Authentication Protocol for IoT and Cloud Servers. Wirel. Commun. Mob. Comput. 2022, 2022, 7707543.

B.D. Deebak (2020), Lightweight authentication and key management in mobile-sink for smart IoT-assisted systems, Sustainable Cities and Society, Volume 63, 102416, ISSN 2210-6707.

Kübra Seyhan, Tu N. Nguyen, Sedat Akleylek, Korhan Cengiz, S.K. Hafizul Islam (2021), Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security, Journal of Information Security and Applications, Volume 58, 102788.

Olakanmi Oladayo Olufemi, Odeyemi Kehinde Oluwasesan (2021), Faster and efficient cloud-server-aided data deduplication scheme with an authenticated key agreement for Industrial Internet-of-Things, Internet of Things, 100376, ISSN 2542-6605.

Mahdi Nikooghadam, Haleh Amintoosi, Saru Kumari, On the Security of “Secure and Lightweight Authentication with Key Agreement for Smart Wearable Systems” Wireless Personal Communications (2021) 120:1–8,2021.

Waseem Iqbal , Haider Abbas , Pan Deng , Jiafu Wan , Member, Bilal Rauf , Yawar Abbas , and Imran Rashid, ALAM: Anonymous Lightweight Authentication Mechanism for SDN-

Enabled Smart Homes, IEEE Internet Of Things Journal, VOL. 8, NO. 12, JUNE 15, 2021.

Sungjin Yu , Ashok Kumar Das , Youngho Park , and Pascal Lorenz, SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments, IEEE Transactions On Vehicular Technology, Vol. 71, No. 10, October 2022.

Priyanka Mall, Ruhul Amin, Ashok Kumar Das, Mark T. Leung, Kim-Kwang Raymond Choo: PUF-Based Authentication and Key Agreement Protocols for IoT, WSNs, and Smart Grids: A Comprehensive Survey. IEEE Internet Things J. 9(11): 8205-8228 (2022)

Man Chun Chow, Maode Ma, A lightweight traceable D2D authentication and key agreement scheme in 5G cellular networks, Computers and Electrical Engineering, Volume 95, October 2021, 107375.

MinahilRana, Akasha Shafiq, Izwa Altaf, Mamoun Alazab, Khalid Mahmood, Shehzad Ashraf, Chaudhryc Yousaf BinZikria, A secure and lightweight authentication scheme for next generation IoT infrastructure, Computer Communications, Volume 165, 2021, pp. 85-96.

Anil Kumar Sutrala, Mohammad S. Obaidat, Sourav Saha, Ashok Kumar Das, Mamoun Alazab, Youngho Park: Authenticated Key Agreement Scheme With User Anonymity and Untraceability for 5G-Enabled Softwarized Industrial Cyber-Physical Systems. IEEE Trans. Intell. Transp. Syst. 23(3): 2316-2330 (2022).

Xinghui Zhu, Zhong Ren, Ji He, Baoquan Ren, Shuangrui Zhao, and Pinchang Zhang, LAAP: Lightweight Anonymous Authentication Protocol for IoT Edge Devices Based on Elliptic Curve, Wireless Communications and Mobile Computing Volume 2022.

Chien Ming Chen, Xiaoting Deng, Wensheng Gan, Jiahui Chen, S. K. Hafzul Islam A secure blockchain based group key agreement protocol for IoT, The Journal of Supercomputing , 1-12, 2021.

B.D. Deebak (2020), Lightweight authentication and key management in mobile-sink for smart IoT-assisted systems, Sustainable Cities and Society, Volume 63, 102416, ISSN 2210-6707.

Kübra Seyhan, Tu N. Nguyen, Sedat Akleylek, Korhan Cengiz, S.K. Hafızul Islam (2021), Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security, Journal of Information Security and Applications, Volume 58, 102788.

Olakanmi Oladayo Olufemi, Odeyemi Kehinde Oluwasesan (2021), Faster and efficient cloud-server-aided data deduplication scheme with an authenticated key agreement for Industrial Internet-of-Things, Internet of Things, 100376, ISSN 2542-6605.

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.

A. Singh, A.N.Tentu, V.Ch. Venkaiah. "A Dynamic Key Management Paradigm for Secure Wireless Ad Hoc Network Communications", International Journal of Information and Computer Security, Volume 14,Nos. 3/4, pp. 380-402, (2021).

Shen, M.; Liu, H.; Zhu, L.; Xu, K.; Yu, H.; Du, X.; Guizani, M. Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE J. Sel. Areas Commun. 2020, 38, 942–954.

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.

Bracciale, L.; Loreti, P.; Pisa, C.; Shahidi, A. Secure Path: Block-Chaining IoT Information for Continuous Authentication in Smart Spaces. IoT 2021, 2, 326–340.

Ferreira, C.M.S.; Garrocho, C.T.B.; Oliveira, R.A.R.; Silva, J.S.; Cavalcanti, C.F.M.D.C. IoT Registration and Authentication in Smart City Applications with Blockchain. Sensors 2021, 21, 1323.

Hameed, K.; Garg, S.; Amin, M.B.; Kang, B. A formally verified blockchain-based decentralized authentication scheme for the Internet of things. J. Supercomput. 2021, 77, 14461–14501.

Narayanan, U.; Paul, V.; Joseph, S. Decentralized blockchain based authentication for secure data sharing in Cloud-IoT. J. Ambient. Intell. Humaniz. Comput. 2021, 13, 769– 787.

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.

Algarni, S.; Eassa, F.; Almarhabi, K.; Almalaise A.; Albassam, E; Alsubhi, K.; Yamin, M. Blockchain-Based Secured Access Control in an IoT System. Appl. Sci. 2021, 17, 1772.

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 Secur. Priv. Cloud IoT 2019, 7, 182772–182783.

Malani, S.; Srinivas, J.; Das, A.K.; Srinathan, K.; Jo, M. Certificate-Based Anonymous Device Access Control Scheme for IoT Environment. IEEE Internet Things J. 2019, 6, 9762–9773.

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.

Sun, S.; Du, R.; Chen, S.; Li, W. Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain. IEEE Acces 2021, 9, 36868–36878.

Liu, S.; Yu, J.; Xiao, Y.; Wan, Z.; Wang, S.; Yan, B. BC-SABE: Blockchain-aided Searchable Attribute-based Encryption for Cloud-IoT. IEEE Internet Things J. 2020, 7, 7851–7867.

Xu, R.; Chen, Y.; Blasch, E. Decentralized Access Control for IoT Based on Blockchain and Smart Contract. In Modeling and Design of Secure Internet of Things; Wiley: Hoboken, NJ, USA, 2020; pp. 505–528.

Bhatt, S.; Sandhu, R. ABAC-CC: Attribute-Based Access Control and Communication Control for Internet of Things. In Proceedings of the 25th ACM Symposium on Access Control Models and Technologies, Barcelona, Spain, 10–12 June 2020; pp. 203–212.

M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," Comput. Security, vol. 78, pp. 126–142, Sep. 2018.

S. Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System, 2008, https://bitcoin.org/en/bitcoin-paper.

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.
Huang, H.; Lu, S.; Wu, Z.; Wei, Q. An efficient authentication and key agreement protocol for IoT-enabled devices in distributed cloud computing architecture. EURASIP J. Wirel. Commun. Netw. 2021, 2021, 150.