MIAS: An IoT based Multiphase Identity Authentication Server for Enabling Secure Communication

R.H. Aswathy[1*], S. Srithar[2], K. Roslin Dayana[3], Padmavathi[4] and P. Suresh[5]

[1*] Assistant Professor (Sl. G), Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore, India. rhaswathy@gmail.com, Orcid: https://orcid.org/0000-0001-5648-2836

[2] Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andrapradesh, India. sss.srithar@gmail.com, Orcid: https://orcid.org/0000-0001-9479-1883

[3] Assistant Professor, Department of Computer Science and Engineering, RMD Engineering College, Chennai, India. dayana.moncy@gmail.com, Orcid: https://orcid.org/0000-0002-9141-6946

[4] Assistant Professor, Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Chennai, India. a_padmavathi@ch.amrita.edu, Orcid: https://orcid.org/0000-0003-2814-5167

[5] Associate Professor, Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore, India. sps1765@gmail.com, Orcid: https://orcid.org/0000- 0002-6766-8908

Received: July 29, 2023; Accepted: October 02, 2023; Published: November 30, 2023

Abstract

Internet of Things (IoT) provides an imminent floor to exchange information and enhance communication technology using embedded devices that are too sophisticated daily and deployed in diverse fields of life. The colossal volume of sensors employed within IoT application leads to disperse an enormous amount of data in the open air. The rudimentary facet of IoT enabled technologies having the pitfall, security. It is a practical problem in terms of networking, application and communication. Since the resource constraint feature of IoT enabled technology, both security and efficiency can be balanced. The effective algorithm builds over Elliptic Curve Cryptography (ECC) provides an effective solution due to its small key size. The sensor node in this scheme is incorporated with TPM to protect the system in crucial IoT applications. In this proposed work, a three-way authentication factor with key agreement protocol proposed with consecutive phases such as registration, login, authentication, and access control. The security assessment of the proposed scheme with diverse attacks are elaborated and the computation overhead compared with related schemes.

Keywords: IoT, Elliptic Curve Cryptography (ECC), Trusted Platform Module (TPM), Three Way Authentication Factor, Key Agreement Protocol.

Journal of Internet Services and Information Security (JISIS), volume: 13, number: 4 (November), pp. 114-126. DOI: *10.58346/JISIS.2023.I4.008*

*Corresponding author: Assistant Professor (Sl. G), Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore, India.

1 Introduction

Today we have hotfoot working towards the multitude of ubiquitous networked communities; the technology is named IoT. The pervasive technology intends to bind every physical object and formulate the data using a petite resource constraint gadget. In this scenario, an enormous amount of data gathers in multiple objects. The intrusion detection system and location are fragile. The security challenges and the simulation tools are explored by author Mardiana et al. The author Kazi et al discussed the integration of new technologies will produce a new security challenges The Gartner market research in the year 2012 states hyper cycle of IoT discussed by (LeHong 2012). This technology captures a decade to reach its upland primarily due to its security challenges. The end-to-end security for internet-connected devices is essential to shield the data even if it moves out of the coverage of the confined network. The analysis of Forrester listed many burning technologies for securing IoT, which includes Authentication, Network and API security. Communicating, gathering, aggregating, monitoring and partnering the information transferring from the IoT device provide an actionable outline and altering to do the desired work through derived policies. The security analytics of IoT will consequently detect intrusions and IoT-specific attacks unidentified by traditional network security such as IDS and Firewalls. IoT is a buzz word for many specific applications, but no one is precisely figuring out how to cope with the risk. Ge, M. et al. (2017) elaborate a framework for modelling and accessing IoT environment security through well-defined security metrics. Sharma, G. and Kalra, S. (2018) proposed a novel lightweight remote authentication scheme for user in cloud IoT applications to provide robustness against attacks. Hong, S. et al. (2018) designed a consistent classification system based on the electronic information system and IoT environment characteristics. The evolution of IoT in today's market brings fear about data confidentiality because all the gadgets interlinked in a chained fashion. Enormous IoT protocols and standard security mechanisms designed constantly, but they not properly examined to prove their trustworthiness. Sfar, A.R. et al. (2018) presented an overview of the roadmap for security challenges based on a novel cognitive and systematic approach. Kaw, J.A. et al. (2019) proposed a novel secure patient information hiding system using optimal pixel repetitions. A biometric-based security architecture was created by Pirbhulal, S. et al. (2019) for an ECG-based wearable health monitoring system. Using a class-based modelling language and a structured methodology, Mavropoulos, O. et al. (2019) developed a security framework to make security analysis in IoT systems easier. There are numerous use cases accessible to research critical security vulnerabilities of IoT devices and their applications. The main objective of the planned activity is to increase awareness of the present flaws and safety issues. Using the security access token, Hossain, M. et al. (2018) created a security system that ensures user authentication and secure access to resources and services. Using MQTT and ECC approaches, (Lohachab, A. 2019) proposed a simple framework for authentication and authorization in the distributed IoT environment. A. Ostad-Sharif et al proposals of a safe and compact authentication and key agreement system for IoT-based wireless sensor networks was made in 2019. The problems with Internet of Things were explored in (Shat et al., 2018). Sharma et al. (2018) discuss a smart card-based authentication system for cloud-based Internet of Things applications. Shen et al(2018) .'s explanation of wireless BAN's lightweight multilayer authentication. The principles in lower extremity healthcare for individuals with varied sclerosis were reviewed by the author Stolt et al,2020. The location privacy method for Internet of Things services was detailed and its applications were described by Sun et al. in 2017. The Re-classification of Internet security analysis was performed by sunyaev et al,2017. By Sunyaev et al. in 2017, Internet security analysis was reclassified. By Taherdoost et al. (2013), the CIA security triangle in the electronic voting system is discussed. Tournier et al. 2020 explored the security concerns with the generic IoT stack. Turknovic et al. (2014) discuss the user authentication and key agreement strategy for heterogeneous adhoc wireless sensor networks based IoT. The technology

age is a significant component of Uribe-Perez, N. et al smart's grid applications, which control numerous devices from a central place (2017). According to research, 155 million automobiles will be connected by 2025. The development of "smart towns" in metropolitan areas has a significant economic impact, as highlighted by Vermesan, O. and Friess, P. (2014). A Two-factor authentication scheme proposed by Wang, D. et al. (2015) provides superior security and privacy without additional communication cost. The challenges encountered by IoT security are highlighted through several case studies. In one instance, the Mirai botnet attack in 2016 exploited weak security measures in IoT devices, leading to a massive distributed denial-of-service (DDoS) attack on major internet services. (Krebs On Security) Similarly, the Jeep Cherokee hack in 2015 exposed vulnerabilities in the vehicle's connected systems, demonstrating the potential dangers of compromised IoT devices in critical domains. (Wired) Furthermore, the Triton malware attack on a petrochemical plant in 2017 underscored the risks associated with IoT devices in industrial control systems, emphasizing the need for robust security protocols in critical infrastructure. (FireEye) These cases underscore the critical need for comprehensive security measures to mitigate the potential risks posed by IoT devices in various sectors.

2 Architecture of Multiphase Identity Authentication Server

IoT proposes new opportunities and challenges that need to address. The most critical parameter in WSN is resource constraint in nature (limited communication and processing capabilities). A vital challenge in this method is to establish a secure connection for exchanging cryptographic key between the sensor node and desired network. The user must be authenticated by an authority in order to access the desired remote node. Elliptic Curve Cryptography (ECC) is a type of public-key cryptography that relies on the mathematical properties of elliptic curves over finite fields. It is widely used for securing communications and data on various networks, including the Internet of Things (IoT) (Tran, V. D., 2023). ECC provides a high level of security with smaller key sizes compared to other encryption techniques, making it particularly suitable for resource-constrained devices in IoT applications. The algorithm's effectiveness is attributed to its ability to provide secure key exchange, digital signatures, and encryption, ensuring data confidentiality, integrity, and authenticity in IoT systems. Trusted Platform Module (TPM) refers to a specialized hardware component that provides a secure environment for the generation and storage of cryptographic keys and sensitive data. It is commonly used to enhance the security of computing devices by offering features such as secure boot, key management, and hardware-based encryption. In the context of IoT, TPM can be integrated into devices to ensure the integrity of the system and protect it from various attacks, including firmware tampering, unauthorized access, and data breaches. By enabling secure storage and execution of sensitive operations, TPM plays a crucial role in safeguarding IoT devices and enhancing the overall security of IoT networks.

The suggested MIAS's architecture design is shown in Figure 1.

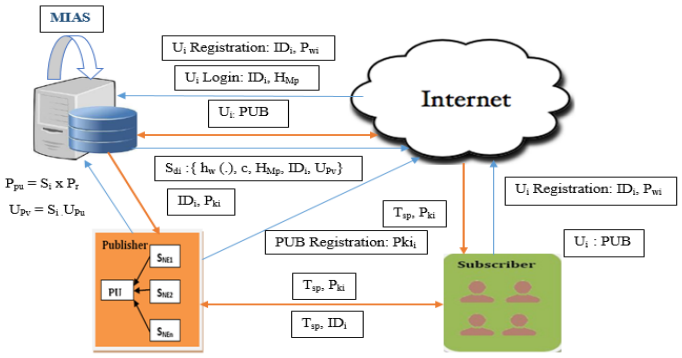

Figure 1: Architecture Diagram of Proposed MIAS

The MIAS architecture has three participants: Users (Ui), Trusted authority (MIAS), Sensor node (S_{NE}) and secure channels (router and internet). The users are the subscribers, doctors, caregivers or family, in the health care system remotely access or monitor the patient's psychological information with the help of MIAS. The S_{NE} is the body sensor node that collects and transfers the data of patient biological information. In order to gather physiological data such as blood pressure, body temperature, heartbeat, body pulse, and electrocardiography, the patient wears body sensors integrated into clothing or devices. Before accessing the system, both users and publishers must register in MIAS. After the successful registration, MIAS issue the smart card and password to the user and the sensor node identity configured with MIAS. The user can communicate with the sensor node are appropriately configured. The timestamp Tsp and sensor node ID is given to the user to access the sensor node. The timestamp Tsp and user identity Pki is given to the sensor node to issue the authorized user information. Both can get identities from MIAS and communicate with each other through a secure channel. Mutual authentication is significant to ensure the entities involved in this communication are legitimate ones. The proposed three-way authentication factor and mutual key agreement protocol using MIAS is most suited for critical healthcare applications. Our schema uses a Smart card (Sdi), Human Memorable password (HMp) and Multiphase Identity Authentication Server (MIAS), a resource-rich server.

Scheme Description

This section set forth an empirical secure three-way authentication factor which includes MIAS, User and node. The security is integrated with MIAS and user through ECC based user authentication via Sdi. The RSA key of node S_{NE} is predominantly stored and secured in MIAS. The proposed server is a resource-rich and trusted authority. The proposed scheme incorporates ECC integrated with Sdi, HMp to enhance provable security.

- **Registration Phase (RP)**

The user sent a registration request to the MIAS with an actual identity. Once the verification has completed, the system administration in MIAS accepts the user to perform the following process. Figure 2 shows the registration phase.

Process RP1: The user Ui selects IDi, Pwi and forwards them to MIAS.

Process RP2: MIAS computes UPv by multiplying S_i and UPu i.e., UPv = S_i *UPu.

Process RP3: To access the session, MIAS uses a random number generator to select the secret parameters c and HMp. The following parameters were created following the registration phase: (hw(.), c, HMp, IDi, and Upv) saved on the smart card Sdi are also transmitted to the Ui in order to protect the communication channel.

User		**MIAS**
User **selects IDi and HMp**	(IDi,HMp) →	MIAS computes UPv UPv =Si.UPu
Ui	← (Sdi) (Via secure channel)	Choose secret parameter c MIAS sent: (hw(.),c,HMp,Idi,UPv)

Figure 2: Registration Phase

- **Login Phase (LP)**

Sdi does the subsequent procedure following the Sdi card is inserted by the user Ui and given the login credentials as user IDi and HMp to login.

Process LP1: Sd_i examines if IDi and HMp given by the Ui are equal with previous stored identity and password. The password matches, proceed to the next step else the verification fails.
Process LP2: If the verification succeeds the MIAS query, the Sd_i computes the signature using 'e', where 'e' is equal to hash of IDi, password HMp.
Process LP3: The Signature Sg computed using $Sg = e.\ UPv$
Process LP4: Sdi posts the message to MIAS through the public communication channel as (Sg, IDi, e, T_{Ln}), where T_{Ln} is the time during the login phase.

- **Authentication Phase (AP)**

After receiving the user's Sg, TLn, c, and IDi login request, MIAS performs the subsequent verification processes. Figure 3 shows the authentication phase.

Process A P 1 : MIAS proceeds Ui's request if the login request message is equal to the IDi stored message at MIAS and evaluate the following: ô (Pr, Sg) =ô (Ppu, e. UPu)

User		MIAS
Ui,Sdi,IDi,HMP	(Ui,Sdi,IDi,HMp) →	Verify MIAS IDi=IDi HMp=HMp Computes e IDi=IDi HMp=HMp then e=h(IDi||HMp||c)
User Ui	(Sg,IDi,e,TLn) ← (via public channel)	Compute Sg Sg=e.UPv

Figure 3: Authentication Phase

Process AP2 : MIAS proceeds next step if it satisfies the following condition time at MIAS $Tnw - TLn < \Delta T$, where Tnw, current time
Process AP3 : MIAS selects a publisher key Pki, incorporates the timestamp sent to the subscriber Ui (Pki, Tsp) to Ui
Process AP4 : All of the nodes, subscribers, and MIAS received the message from (Tsp, IDi), which guarantees that user Ui is an authenticated user. The time limit, Tsp, is calculated here. Within the allotted period, Ui must access the data from the sensor node

- **Access Control (AC)**

The authorized user, Ui, access the data generated from the S_{NE} sensor node within a particular time limit. After getting the authentication for the secure transportation of data, the following steps executed. Figure 4 and 5 shows the access control and message transferring phase respectively.

Process AC1 : Ui inserts Sd_i and gives IDi and HMp. Sd_i equates the values to the stored value to validate Ui and then proceeds.

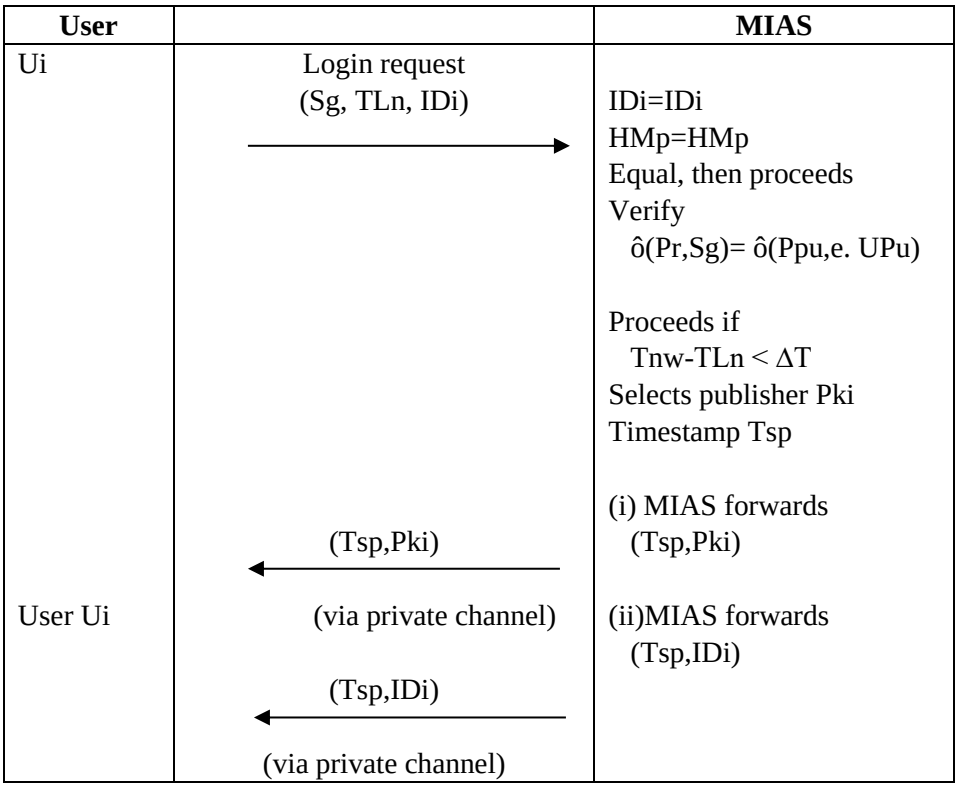

Figure 4: Access Control Phase

Process AC2 : Sd_i evaluates Tsp (timestamp) and Pki (publisher key).

Process AC3 : PUB verifies after receiving the message (T_{sp}, Pki).

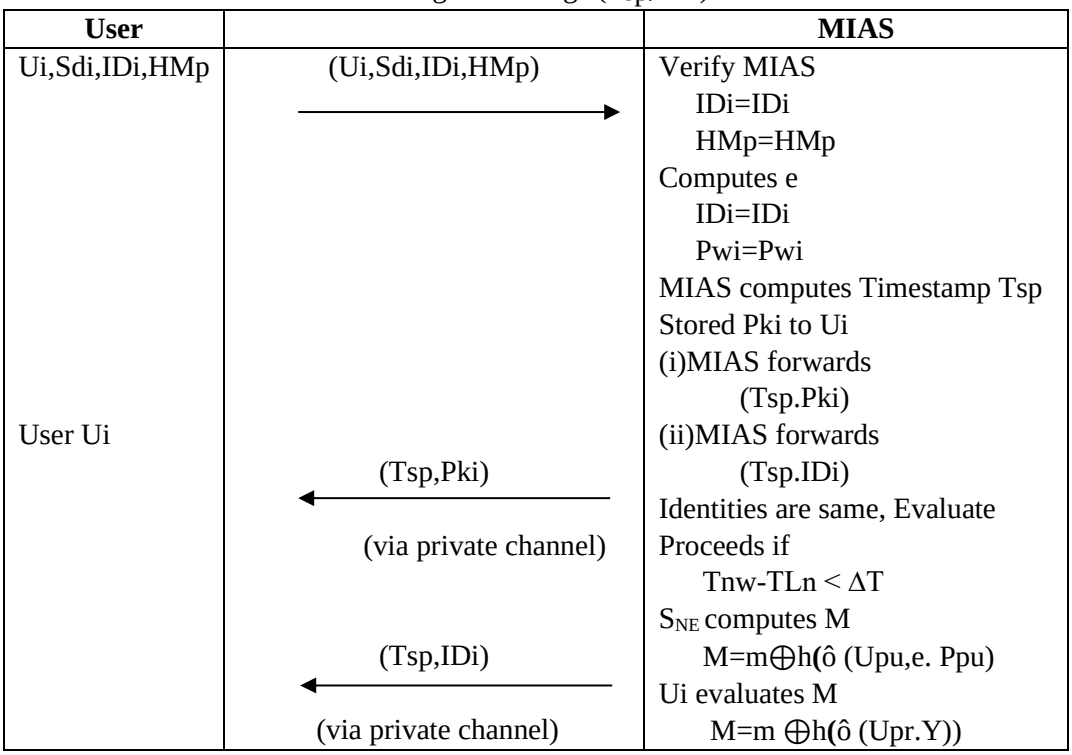

Figure 5: Message Transferring Phase

Process AC4 : The subscriber (user Ui) and the publisher (sensor node S_{NE}) evaluate the timestamp Tsp by checking the following: User Ui: (Tsp, Pki) and Node S_{NE} :(Tsp, IDi)
Process AC5 : The user Ui request the message M, the S_{NE} computes M as M= M ⊕ h(ô (UPu. Ppu))
Process AC6 : Ui retrieves M by evaluating M using M = M ⊕ h(ô (UPr. Y)), where Y is a parameter public to all.

3 Security Assessment of Proposed Scheme

The security assessment of the proposed schemes is discussed. The security of the authorized protocols is essential, but it is not easy to attain. Many devices connected through communication and share information; security plays a crucial role. This scheme shields and contribute to impersonation, user anonymity, stolen smart card, mutual authentication, privileged insider, offline password guessing, DDoS and independent password update attack. Therefore, the proposed MIAS provide secure communication in the case of IoT.

Impersonation Attack

An advisory utilizes some shielded and private information to execute an impersonation attack. The adversary acts as a valid user and impersonates a MIAS. In the proposed scheme, the MIAS is resilient to those attacks because eavesdrop on a valid user authentication is impossible to compute a session key within a particular timestamp and retransmit data to the sensor node. In the discussed schema, the timestamp computed using Tnw - TLn < ΔT. To perform an impersonation attack, the attacker needs to take more time than the actual time required to transmit data. The method used in the proposed work helps to find the actual time and avoid impersonation attack.

User Anonymity

The authentication request processed through a public channel. MIAS server can register the user identity in the initial registration and MIAS computing the private parameter given along with HMp. The private parameter and HMp is unknown to an adversary, so the adversary does not eavesdrop on the secret parameter. During this communication, the identity computed using the MIAS master key. Even a smart card stolen attack may happen; the adversary will not infer the private information of a single user.

Offline Password Guessing Attack

Consider the scenario where an attacker named "A" has obtained all the private data from Ui (hw(.), c, Pwi, IDi, UPv). Due to the one-way nature of the hash function, hw, it is impossible to obtain the HMp of Ui and recover the data of Sdi (.). It hides the importance of c, UPv, and IDi. The suggested approach is hence resistant to the offline password guessing attack.

Stolen Smart Card Attack

Consider the scenario where user Ui loses his or her smart card and an opponent gathers all sensitive data, including (hw(.), c, Pwi, IDi, and UPv. The hash function hw(.) conceals all of the data, and in addition, HMp is a password; it cannot be read without the user's knowledge, therefore the smart card does not reveal any sensitive information about Ui.

Mutual Authentication

The Ui and S_{NE} authenticate mutually with the help of MIAS. Ui computes Sdi with IDi and HMp, Sdi computes timestamp along with IDi. An adversary cannot perform this hash function done by MIAS. Mutual authentication achieved using the robust computation of MIAS.

Privileged Insider Attack

The malicious unauthorized user with valid privilege collects the user's sensitive information and tries to log in to networks where the user has the account. This attack is frequently occurring due to improper logout or system operations. Even though the adversary knows the user name and password, still it requires Sdi to access the data.

DDoS Attack

When a user enters wrong identity and password information during the login process, the smart card (Sdi) uses hw(.), c, HMp, IDi, and UPv to validate the user's credentials. This function works based on the correct user credentials, so the DDoS will not occur with invalid user credentials. The attacker may also try to engage the sensor node by continuously sending the message to delay the valid user login attempt. Here the transmitted message is given with the timestamp TLn (Time to login). Using the timestamp, the sensor node confirms the message's freshness (Tsp, Pki). The sensor node is informed by the delayed message that the request is a fraudulent one. The illustration demonstrates how the suggested approach withstood a DDoS attack.

Independent Password Update

The MIAS would like to change the password, and the subsequent communication of user Ui will change the particular master key in the smart card Sdi without any conflict or delay. This MIAS secret password will increase the security of the proposed system. This scheme must strongly support the strong HMp using a random number generation algorithm. In this proposed generator, ECC over a finite field is chosen and incorporate the initial seed value with the KnP module is a prime number with the order of Infinity 'O'. The generated password could easily share through a private channel during registration.

4 Experimental Evaluation and Observation

The focus of the suggested plan is an IoT-based, smart card-based security-enabled system. Additionally, it was created so that a distant user could utilise a smart card that included IDi and HMp to connect directly with the sensor node. After logging in, the Trusted Platform Module strongly safeguarded the sensor node associated with the suggested scheme. The suggested scheme's performance is evaluated in terms of its security features and computational overhead in comparison to similar systems. The outcome demonstrates that, in comparison to other systems, the suggested method is very effective.

Comparison of Security Features

Comparing the security attributes of various methods is shown in Table 1. Attacks like impersonation attacks, user anonymity attacks, offline password guessing attacks, attacks using stolen smart cards, mutual authentication attacks, attacks using privileged insiders, DDoS attacks, and attacks using MIAS independent password are taken into consideration and compared with related schemes. The analysis made here clearly indicates that the proposed model provides better security and additional functionality of smart cards, and private parameters makes the system more efficient. It observed that the proposed scheme provide a notable improvement when compared to the existing schemes.

Table 1: Comparison of Security Features

Attacks/Schemes	MIAS	Li, C.T. et al. (2017)	Wu, F. et al. (2015)	Arshad, H. and Nikooghadam, M. (2014)
Impersonation attack	√	×	×	√
User anonymity	√	×	√	√
Offline password guessing attack	√	×	√	√
Stolen smart card attack	√	×	√	×
Mutual authentication	√	×	√	√
Privileged insider attack	√	√	√	√
DDoS attack	√	√	×	√
Independent password update	√	√	×	×

Comparison of Computation Cost

The computation cost of the proposed scheme compared with other related schemas. Consider a sensor node identity S_{NE} Random number generator, timestamp, hashing technique and Elliptic curve cryptography point pt= (Pi, Pj). In general, the 1024 bit of RSA public key cryptosystem is equal to 160-bit of elliptic curve cryptography. Compared to other relevant schemas, the computing cost of the suggested method. Consider the the sensor node identification SNE Random number generator, timestamp, hashing method, and elliptic curve cryptography point pt= (Pi, Pj). Generally speaking, the 160-bit elliptic curve cryptography is equivalent to the 1024-bit RSA public key cryptosystem. Summing the cost of all the parameters (IDi, HMp, hw(.), TLn) of login phase, authentication and verification phase is better than all available schemes.The approximate time needed to complete the cryptographic processes is shown in Table 2. The cryptographic operations include symmetric encryption/decryption, bilinear pairing, ECC point multiplication and hash function. As per the author He, D., et al. (2014) discussion, the computation time for ECC calculated as Tm≈Tecm/400.

Table 2: Time Required for Performing Cryptographic Operations

Approximate time required for various operations		
Tsym	Symmetric encryption/decryption	0.0056
Tbp	Bilinear pairing	0.0045
Tecm	ECC point multiplication	0.0171
Tn	Hash function	0.00032

The comparison of calculation overhead for various strategies is shown in Table 3. The hash function, ECC point multiplication, and bilinear pairing calculation overhead are all calculated. The suggested approach is demonstrated to have low overhead and high efficiency by the user Ui, Sensor node SNE, and computation in MIAS, which together account for less overhead of roughly equal to 0.06576s. The comparison of communication overhead with related methods is shown in Figure 6.

Table 3: Comparison of Computation Overhead with Different Schemes

Schemes	User Ui	Server	Sensor node S_{NE}	Cumulative overhead
Li, C.T. et al. (2017)	$3T_h+1T_{bp}+2T_{ecm}$	$1T_h+2T_{bp}$	$3T_h+1T_{bp}$	≈0.5444 s
Wu, F. et al. (2015)	$5T_h+1T_{fe}+2T_{ecm}+2_{sym}$	$6T_h+2T_{sym}+2T_{ecm}$	-	≈0.11142s
Arshad, H. and Nikooghadam, M. (2014)	$3T_h+1T_m+2T_{ecm}$	$1T_{inv}+7T_h+1T_m+2T_{ecm}$	-	≈0.07327s
MIAS	$1T_h+1T_{ecm}$	$1T_h+1T_{bp}+1T_{ecm}$	$1T_h+1T_{bp}$	≈0.06576s

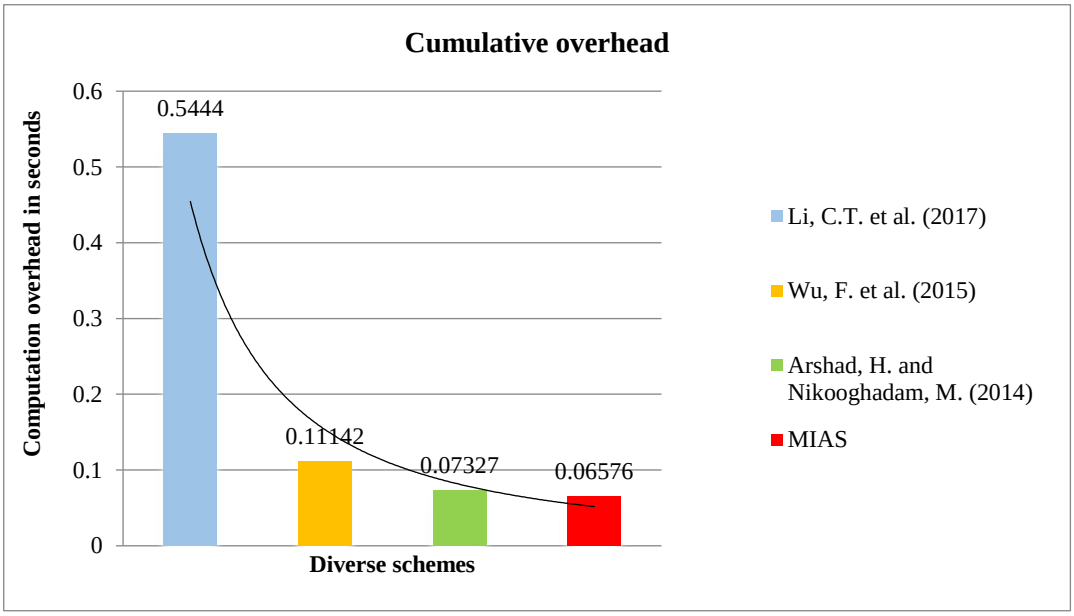

Figure 6: Comparison of Computation Overhead with Proposed Scheme

5 Conclusion

The implementation of a three-way authentication factor in IoT-enabled applications serves as a robust security mechanism to ensure secure communication within the IoT network. Incorporating this three-way authentication factor along with Trusted Platform Module (TPM) within the sensor node introduces notable security enhancements, highlighting its superiority over existing security schemes. The comprehensive evaluation of the proposed system demonstrates its resilience against various well-known attacks, including but not limited to impersonation, user anonymity, offline password guessing, stolen smart card, mutual authentication, privileged insider, distributed denial-of-service (DDoS), and independent password update attacks. Furthermore, the proposed system effectively fulfills the majority of security requirements while maintaining a high level of computational efficiency, effectively striking a balance between ensuring robust security measures and optimizing system performance.

References

[1] Ge, M., Hong, J.B., Guttmann, W., & Kim, D.S. (2017). A framework for automating security analysis of the internet of things. *Journal of Network and Computer Applications*, *83*, 12-27.

[2] Hassan, W.H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, *148*, 283-294.

[3] Hong, S., Park, S., Park, L.W., Jeon, M., & Chang, H. (2018). An analysis of security systems for electronic information for establishing secure internet of things environments: Focusing on research trends in the security field in South Korea. *Future Generation Computer Systems*, *82*, 769-782.

[4] Hossain, M., Islam, S.R., Ali, F., Kwak, K.S., & Hasan, R. (2018). An Internet of Things-based health prescription assistant and its security system design. *Future generation computer systems*, *82*, 422-439.

[5] Kaw, J.A., Loan, N.A., Parah, S.A., Muhammad, K., Sheikh, J.A., & Bhat, G.M. (2019). A reversible and secure patient information hiding system for IoT driven e-health. *International Journal of Information Management*, *45*, 262-275.

[6] LeHong, Hype Cycle for Internet of Things, 2012, Tech. Rep., Gartner Inc. (2012).
[7] Lohachab, A. (2019). ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. *Journal of Information Security and Applications*, *46*, 1-12.
[8] Mavropoulos, O., Mouratidis, H., Fish, A., & Panaousis, E. (2019). Apparatus: A framework for security analysis in internet of things systems. *Ad Hoc Networks*, *92*, 1-18.
[9] Ostad-Sharif, A., Arshad, H., Nikooghadam, M., & Abbasinezhad-Mood, D. (2019). Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme. *Future Generation Computer Systems*, *100*, 882-892.
[10] Pirbhulal, S., Samuel, O.W., Wu, W., Sangaiah, A.K., & Li, G. (2019). A joint resource-aware and medical data security framework for wearable healthcare systems. *Future Generation Computer Systems*, *95*, 382-391.
[11] Sadique, K.M., Rahmani, R., & Johannesson, P. (2018). Towards security on internet of things: applications and challenges in technology. *Procedia Computer Science*, *141*, 199-206.
[12] Sfar, A.R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118-137.
[13] Sha, K., Wei, W., Yang, T.A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. *Future generation computer systems*, *83*, 326-337.
[14] Sharma, G., & Kalra, S. (2018). A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications. *Journal of information security and applications*, *42*, 95-106.
[15] Shen, J., Chang, S., Shen, J., Liu, Q., & Sun, X. (2018). A lightweight multi-layer authentication protocol for wireless body area networks. *Future generation computer systems*, *78*, 956-963.
[16] Stolt, M., Laitinen, A.M., Ruutiainen, J., & Leino-Kilpi, H. (2020). Research on lower extremity health in patients with multiple sclerosis: a systematic scoping review. *Journal of foot and ankle research*, *13*(1), 1-17.
[17] Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H., & Liao, D. (2017). Efficient location privacy algorithm for Internet of Things (IoT) services and applications. *Journal of Network and Computer Applications*, *89*, 3-13.
[18] Sunyaev, A., Tremmel, F., Mauro, C., Leimeister, J.M., & Krcmar, H. (2009). A reclassification of is security analysis approaches.
[19] Taherdoost, H., Chaeikar, S., Jafari, M., & Shojae Chaei Kar, N. (2013). Definitions and criteria of CIA security triangle in electronic voting system. *International Journal of Advanced Computer Science and Information Technology (IJACSIT) Vol*, *1*, 14-24.
[20] Tournier, J., Lesueur, F., Le Mouël, F., Guyon, L., & Ben-Hassine, H. (2021). A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things*, *16*.
[21] Tran, V. D., Le, P. T., & Trinh, V. C. (2023). A Secure Proxy Re-Signature Scheme for IoT. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *14*(1), 174-188.
[22] Turkanović, M., Brumen, B., & Hölbl, M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Networks*, *20*, 96-112.
[23] Uribe-Pérez, N., Angulo, I., De la Vega, D., Arzuaga, T., Fernández, I., & Arrinda, A. (2017). Smart grid applications for a practical implementation of IP over narrowband power line communications. *Energies*, *10*(11), 1-16.
[24] Vermesan, O., & Friess, P. (2014). *Internet of things applications-from research and innovation to market deployment*, 364. Taylor & Francis.
[25] Wang, D., Wang, N., Wang, P., & Qing, S. (2015). Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity. *Information Sciences*, *321*, 162-178.

Authors Biography

Dr.R.H. Aswathy, is an Assistant Professor (Sl. G) in the Department of Computer Science and Engineering since June 2017. She obtained her B.E (CSE) from Narayanaguru Engineering College (Anna University, Chennai) and M.E (CSE) from Karpaga vinayaka college of Engineering and Technology (Anna University, Chennai). She completed her PhD in Vel Tech Rangarajan Dr Sagunthala R & R&D Institute of Science and Technology, Chennai. She has been in the teaching profession for the past 11 years and has handled both UG and PG programmes. Her area of research includes IoT and Artificial Intelligence. She received NPTEL Dicipline star award in 2021. She received the faculty partnership model award-bronze level twice from Infosys in the year 2016 and 2017. She has published four books and published seven research papers in International Journals and seven papers in International and National Conferences. She has attended many workshops & FDPs sponsored by AICTE related to her area of interest. She is a lifetime member of IAENG and ISTE.

Dr.S. Srithar is working as Associate Professor in the Department of Computer Science and Engineering at KL University, Andhra Pradesh. He Completed his Ph. D in computer science and Engineering from Anna university, Chennai and completed his M. Tech Information Technology and B.E computer Science and Engineering from PSN College of Engineering and Technology, Tirunelveli under anna university. He has totally 9 years of experience in teaching. He has published more than 50 research articles in scopus and SCI indexed journals/conferences/book chapters. He has 3 international patent publication. He organized and attended more than 100 FDPs/Workshops/Webinars. He is specialized in modern web development tools like React, Node JS, Angular and Mongo DB. He established an EMC Bigdata Analytics Lab in collaboration with ICTACT academy. He also acted as resource person for the FDP, workshop, and conferences across India. He is a certified Microsoft Azure Associate certified cloud trainer. He is currently working towards 4 consultancy projects and completed one CSIR funded workshop. He is specialized in cloud domains such as AWS and Microsoft Azure. He has received his special commendation for produced 100% results in 3 Academic years continuously and IIT Bombay commendation for spreading spoken tutorial projects across the students. He is a life member of ISTE, IAENG and ISRD.

Ms. Roslin Dayana K is working as Assistant professor in RMD Engineering College. She has 12 years of teaching experience. She has completed B.E. Computer Science and Engineering in Dr. Navalar Nedunchezhiyan College of Engineering, Cuddalore and M.E. Computer Science and Engineering in Veltech Engineering College, Chennai. Her areas of research interest include Cloud Computing, Big Data, Distributed Database and Data Science. She is pursuing Ph.D. in Cloud Computing under Anna University. She has presented papers in National and International conferences and also published papers in journals. She has participated in various Anna university organized workshops and completed multiple AICTE organized FDPs. She also has completed online MOOC courses related to her areas of interest.

Dr. A. Padmavathi currently serves as an Assistant Professor (Selection Grade) at the Department of Computer Science Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Chennai Campus. She obtained her B. E. (CSE) from Periyar Maniammai College of Technology for Women, Vallam, in 1999 and M. E. (Software Engineering) from Anna University in 2006. She received her Ph. D. in the area of P2P Networking from Anna University, Chennai, in 2016 She has been in the teaching profession for over 24 years and has guided various UG and PG projects and currently guiding 3 Ph.D. research Scholars. Her research interests include Programming, Computer Networks, Networks Security, Cyber Security, Soft Computing, P2P Networks, Distributed Computing, IOT, Block Chain Technology, Machine Learning. She has published many research papers in various International Journals and Conferences and has attended many workshops and FDPs sponsored by AICTE related to her area of interest. She is a life member of IAENG and ISTE.

Dr.P. Suresh is an Associate Professor in the Department of Computer Science and Engineering at KPR Institute of Engineering and Technology. He was associated with Vel Tech Multi Tech Dr Rangarajan Dr Sakunthala Engineering College, Chennai. He obtained his B. Tech (IT) from Vel Tech Engineering College (Anna University, Chennai) and M. E (CSE) from Vel Tech Multi Tech Dr Rangarajan Dr Sakunthala Engineering College (Anna University, Chennai). He did his PhD in Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Chennai. He has been in the teaching profession for the past 15 years and has handled both UG and PG courses. His area of research is the Internet of Things (IoT) and Machine Learning. He has published three books, 15 research articles in International Journals and has presented ten papers in International and National Conferences. He has attended various Training Programmes, Workshops and Faculty Development Programmes sponsored by AICTE related to his interest area. Recently, the students won the Project Innovation Awards for IoT project under his guidance in various contests and have applied for a patent for the same. He is a lifetime member of IAENG and ISTE.