Secure & Efficient Authentication Framework for Internet of Things

Palak Patel[1*], Dr. Chintan Shah[2], Dr. Premal Patel[3]

[1*,2,3]Aditya Silver oak Institute of Technology, Silveroak University, Ahmedabad.
Palakpatel.rs@silveroakuni.ac.in

Abstract
The Internet of Things (IoT) is collection of all interrelated physical devices that are able to communicate with each other without the need for human, system or computer interference. When packaged right, IoT has the power to transform industries like healthcare, agriculture, and smart cities by delivering better, smoother, and efficient services, however, the interconnected framework of IoT also provides opportunities for significant security breaches. These vulnerabilities may be exploited by adversaries to achieve several different scenarios, including replay attacks, man-in-the-middle (MITM) attacks, and location spoofing. The resource constraints of IoT devices mean normal cryptographic solutions are inappropriate. So, in this paper we introduce a lightweight and secure multifactor authentication protocol for IoT environment. The proposed protocol provides a strong protection against replay, MITM, and other cyber threats while keeping a low computational and communication overhead. It provides formal analysis of the security of the protocol using tools such as AVISPA and SPAN, which serve to verify that the protocol is resistant to different types of attacks. Our findings show that the proposed mechanism not only provides an additional security level compared to previous approaches but also represents an efficient solution for real-world IoT settings.

Keywords: *Internet of Things (IoT), Multi-factor Authentication, Replay Attacks, Man-in-the-Middle (MITM), Lightweight Protocol, Cybersecurity, Formal Verification, AVISPA, SPAN*

Introduction

The Internet of Things (IoT) is a revolutionary technological framework consisting of billions of interconnected devices communicating and sharing data autonomously. The Internet of Things (IoT not only connects computers and servers to the Internet, but also physical devices, which can communicate with each other and dispense information as needed. Its usage extends over a variety of industries, such as healthcare, agriculture, smart cities, transportation, industrial automation, and more. The Internet of Things has also proven invaluable for healthcare, notably for monitoring patients in remote areas with limited medical infrastructure. It enables recurrent patient monitoring at the house and allowing healthcare professionals to quickly respond to crises, increasing essential care.

There are few key components through which IoT works that are given below:
Sensors: Capture physical properties and features.
Annotation: Provide a store and manage data.
Connects: Enables interaction among devices.
Applications: Storage & processing in a cloud service or database.
Decision Trigger: Allow users to experience application and interact with it outcome.
This system will provide aid for improving sectors, transforming system level process and enhance the living standards of the nation.
IoT is primarily used to improve efficiency in the real world, usage of the resources and effective decision-making systems.

IoT Security

Authentication: Authentication In IoT: this ensures that only legitimate users and devices can access the network and the resources it manages. This includes confirming user, system, or device identity using methods like passwords, biometrics, or digital certificates. More sophisticated approaches, such as multi-factor authentication (MFA) which requires several proofs of identity, further bolster security. [36] which is critical for preventing devices from entering the IoT (internet of thing) devices [36] and facilitating authenticated devices' trustworthiness in the system. When authentication is not implemented properly, attackers will be able to pose as genuine devices or users connected to the network and take advantage of the system, resulting in system violations and misuse.

Encryption: Encryption protects data in transit and at rest and is a key aspect of IoT security. This allows only those with proper decryption keys to access the data, as they are no longer written in a readable format. IoT systems use data encryption protocols like TLS (Transport Layer Security) and AES (Advanced Encryption

Standard) to protect data communication. It guarantees that the data remains unreadable and untampered even if an attacker intercepts it. In sensitive IoT use cases such as healthcare and finance, proper encryption is essential, as confidentiality and integrity of the data are critical.

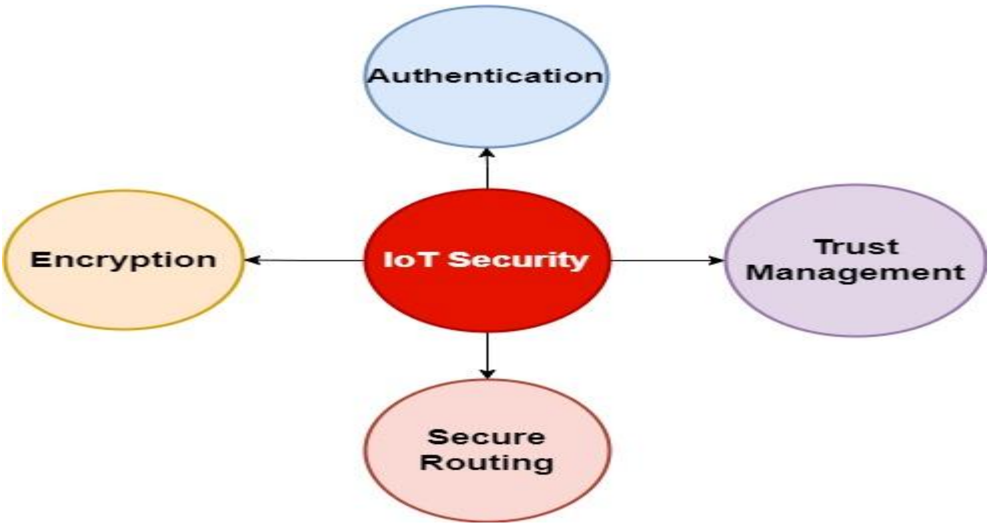


Figure 3: IoT Security

Secure Routing: Secure routing in IoT refers to the process of securing paths through which data is transmitted from a sensor, actuator, or another IoT device, to a gateway and then to a server. It ensures that data is transferred to the right destination without intercepting, changing, or redirecting it. A secure routing protocol is used to identify and eliminate attacks (e.g., sinkhole attacks (where malicious nodes lure and discard data packets), blackhole attacks that entirely disables data transfer). Secure routing ensures that malicious activities do not affect the continuous communication of the IoT for efficient communication of opportunistic networks.

Trust Management: A review of existing approaches and challenges It creates trust scores for devices depending on their behavior and interaction history. Low trust score devices may be limited or isolated from the network to minimize risk, while you reserve full access for high trust score devices. Empower and build trust management to help identify compromised/rogue devices to enable only trusted operation within the sensing network. It supposes that all peers are authenticated and trustworthy, accelerating the performance of IoT system security.

IoT Authentication and Types

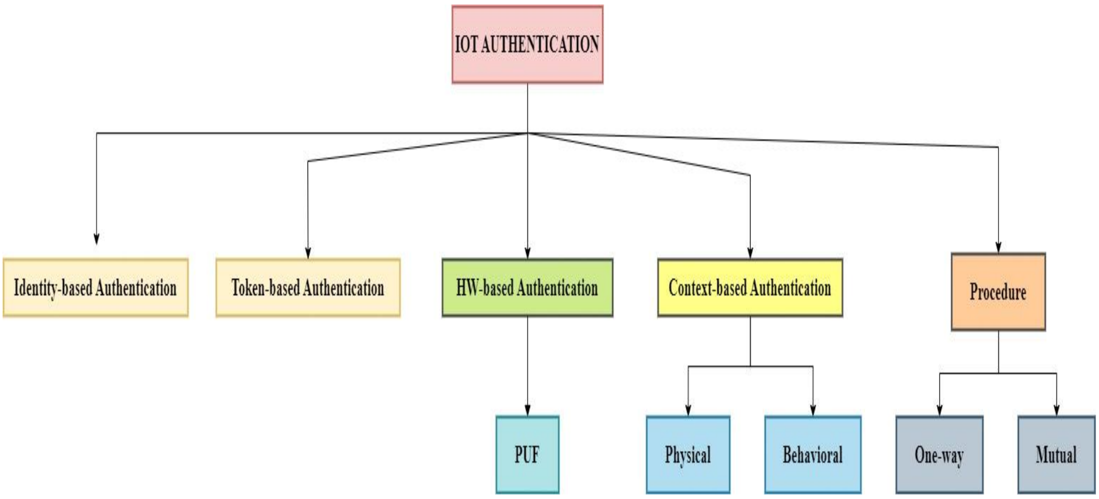


Figure 2: IoT Authentication and Types

Classification of IoT authentication methods, divided into different categories based on their approach. It starts with IoT Authentication as the central concept, which branches out into Identity-based Authentication, Token-based Authentication, HW-based Authentication, Context-based Authentication, and Procedure.

1. Identity-based Authentication ensures devices or users are who they claim to be by verifying their identity.
2. Token-based Authentication uses a unique token as proof of identity for authentication purposes.
3. HW-based Authentication relies on hardware components, such as PUF (Physical Unclonable Functions), to enhance security.
4. Context-based Authentication is based on the context or behavior of the user or device, further split into:
   - Physical (e.g., location-based).
   - Behavioral (e.g., patterns of interaction).
5. Procedure refers to two types of methods:
   - One-way Authentication, where one party proves their identity.
   - Mutual Authentication, where both parties authenticate each other.

Literature Review

Sr. No.	**Authors**	**Proposed Technique**	**Findings**
1.	Poornima Nag et al. (2023)	Two Factor based authentication schema: User Id-Password, Smart Card	1. Does not provide User Anonymity as User ID is transferred to the Medical Server in the Registration Request. 2. The user's smart card contains users' valuable information, it can be fetched by power analysis attack and further attack can be possible. 3. Proposed schema is vulnerable to Smart Card Stolen, Password guessing threats.
2.	Chia Hui Liu et al, (2021)	Proposed reliable authentication schema is based on: Password & Smart Card.	1. In Initial Phase, every User has to do the registration with the Central Authority (CA). CA computes the Public Key for each user and it will be stored on the Smart Card. So, there is a possibility of Single Point Bottleneck if there will be any attack on CA. All users Public key can be stolen and misused in the future. 2.In Registration Phase, Users do the registration with CA by using User ID and Password. Registration Request = { User ID, User Password}. So, this registration message can be captured and modified. In future Replay attack, MITM attack, impersonate attack is possible. There should be any secure channel/ method be developed for transmission of this Registration Message.
3	Ravi Chaudhary et al, (2020)	Mutual Authentication Protocol: Challenge-Response, Diffie –hellman key exchange method	1. For the session key generation, Diffie-Hellman Key Exchange Method is used. It is asymmetric cryptography method. IoT is resource constrained network, Asymmetric Cryptography is required more computational tasks because of that network lifetime can be limited. MITM attack is possible in suggested method.

4	Swati Laxmeshwar et al. (2020)	An efficient authentication schema based on Blockchain technology is suggested. Proposed approach provides data integrity also.	1. High processing power required for Proof of work 2. Storage too will be a hurdle. Blockchain eliminates the need for a central server to store transactions and device IDs, but the ledger has to be stored on the nodes themselves. And the ledger will increase in size as time passes. That is beyond the capabilities of a wide range of smart devices such as sensors, which have very low storage capacity. 3. Mining of blocks is time consuming while in most IoT applications low latency is desirable
5	Sanjukta Das et al., (2023)	PUF based Authentication Method	Communication Interception is possible at the time of exchanging Challenge-Response. Modelling attack is also possible in PUF based approach. PUF Response can vary for the same challenge based on Environmental Conditions including Voltage & Temperature.
6	Fei Tang et al. (2019)	Block chain-based Authentication Method	Higher Resource consuming: Processing power, storage 2. Scale poorly with large number of nodes in the network. 3. High bandwidth requirements
7	Naba Hamid et al. (2022)	Secure Patient Authentication Method Based on One Time Pad & Symmetric Encryption	No any method is explained about the key generation with OTP Method. If Domain is of small range then Dictionary Attack/ Key Guessing Attack is possible. Once Key is guessed, further attacks such as Modification, Impersonate, MITM are also possible. No any description about the Key Exchange between the Patient and EHR Server.

Research Gap

Most of the existing Authentication methods for EHR Authentication use a single key-based approach / password-based approach to authenticate the participated entity of the network. From the literature survey we found that such kinds of the methods are vulnerable to the different attacks such as Key stolen attack, Side channel attack, MITM attack, Device cloning attack. Most of the methods uses same password for the entire life cycle of the network for authorization purposes. If the password also not changed over the time, then also it is prone to Dictionary attack. And if the adversary has the shared key/password, an identical fake device also can be made.

So, there is a need to work on authentication approach in which key value should be changed over the time. So, if adversary gets shared key than also, he/she cannot get access of the system and cannot compromise with system security. We can provide security against MITM attack, Interception attack, Dictionary attack, Key stolen attack, Device cloning attack and Replay attack. Designed Authentication method also must be Mutually Authentication based Method. In which identity of HER Server also should be verified with the identity of participant entities such as various sensor nodes & users. It will enhance the security for the network.

Methodology of Research Gap

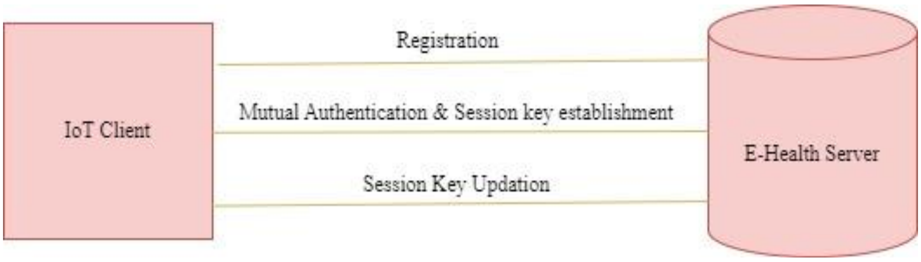


Figure 4: Proposed Model

The in figure demonstrates the interfacing of an IoT Client with an E-Health Server, wherein the three essential mechanisms taking place are outlined which assures the secured communication and data transfer between the Client and Server.

Registration: The IoT client registers with the E-Health server by advertising its identity and credentials, which the server verifies to allow access. This ensures only authorized devices can join the network.

Mutual Authentication and Session Key Establishment: Both the IoT client and server authenticate each other to prevent impersonation. A secure session key is established to encrypt communications, ensuring confidentiality and integrity.

Session Key Updating: To maintain security over time, the session key is frequently refreshed. This prevents future communications from being compromised, even if an earlier key is exposed.

Proposed System

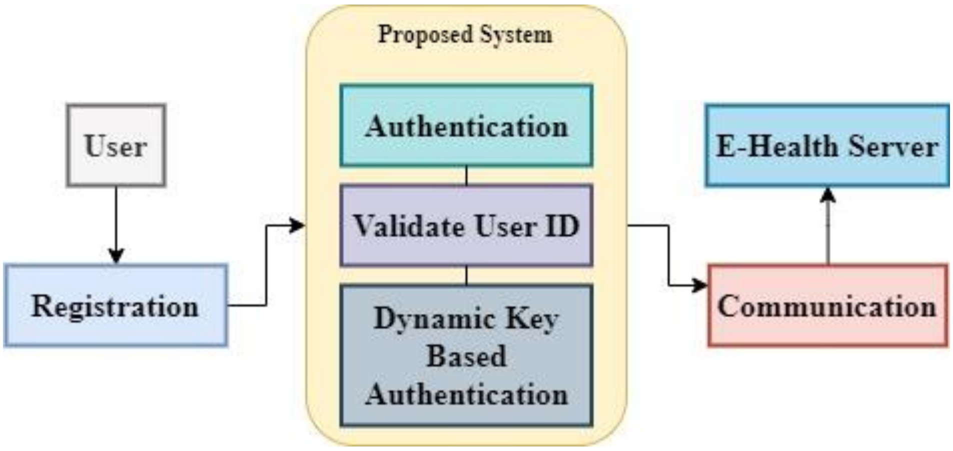


Figure 5: Proposed Model

Steps

Step 1: Registration

- The user initiates registration with the E-Health Server.

Step 2: Authentication

- The registered user sends a **login request** along with their **current session ID** to the server.
- This step verifies that the user is actively attempting to access the system.

Step 3: User ID Validation

- The E-Health Server checks the **User ID** for validity:
  - **If Valid**: The system authenticates the user and allows them to proceed.
  - **If Invalid**: The session is immediately terminated, and the activity is flagged as potentially malicious.

Step 4: Dynamic Key-Based Authentication

- For valid users, the system generates a **dynamic session key** for encryption.
- This ensures secure, session-specific authentication and data exchange.

Step 5: Communication

- Once authenticated, the user is granted access to the E-Health Server.
- A secure communication channel is established to allow safe exchange of sensitive health data.

Notation	Description
||	Concentation Operation
⊕	Ex-OR Operation
h	Message Digest Function
Random Number	64-bit Random Number for Mutually Authentication Purpose
Temporary Number (Nonce)	64-bit Random Number for Session Key Generation Purpose

Table 1: Notation Table

Proposed System with AVISPA

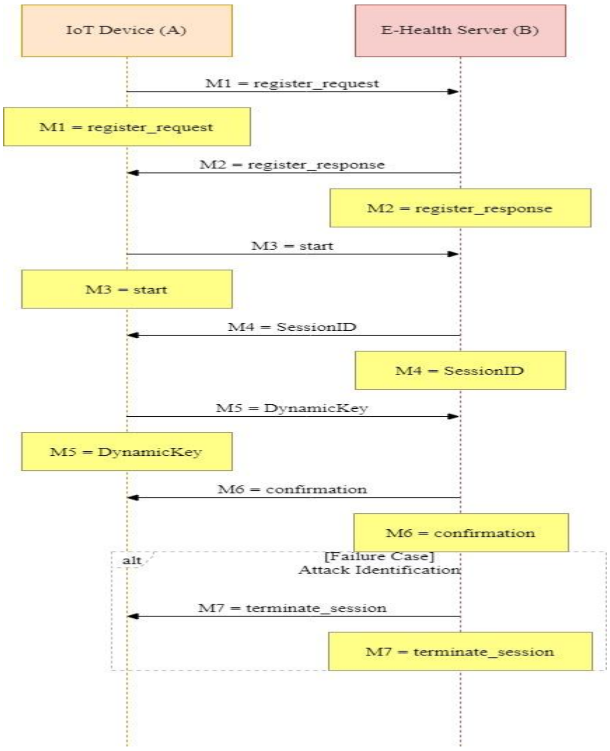


Figure 6: Message Exchange between Dynamic Key based Authentication

This flow ensures secure mutual authentication between an IoT device and an E-Health server, protecting data confidentiality, integrity, and against cyber threats. It starts with the IoT device registering with the server, which generates a unique session ID for secure communication. Dynamic key exchange is used, ensuring a new encryption key for every session. Mutual authentication is achieved through cryptographic operations, preventing unauthorized access. Nonces and symmetric XOR functions are employed to prevent replay attacks. The flow includes attack detection mechanisms to terminate sessions when malicious activity is detected.

The benefits include mutual authentication, unique encryption keys, and protection against replay and MITM attacks. Cryptographic operations ensure data confidentiality and integrity, while the lightweight protocol is suitable for resource-constrained IoT devices. The scalable design is applicable to E-Health systems, ensuring secure communication and compliance with IoT security standards for sensitive health data.

Author Consider Tools like AVISPA (Automated Validation of Internet Security Protocols and Applications) is a formal verification tool commonly used to analyze and verify communication protocol properties. AVISPA works by modelling protocol interactions in a formal model and verifying the absence of threats like replay attacks, man-in-the-middle attacks, and others. And multi-backend support (OFMC, CL-AtSe) for security protocol analyser.

PROTOCOL: Dynamic Key based Mutual Authentication Protocol

VARIANT: Two-Pass Mutual Authentication

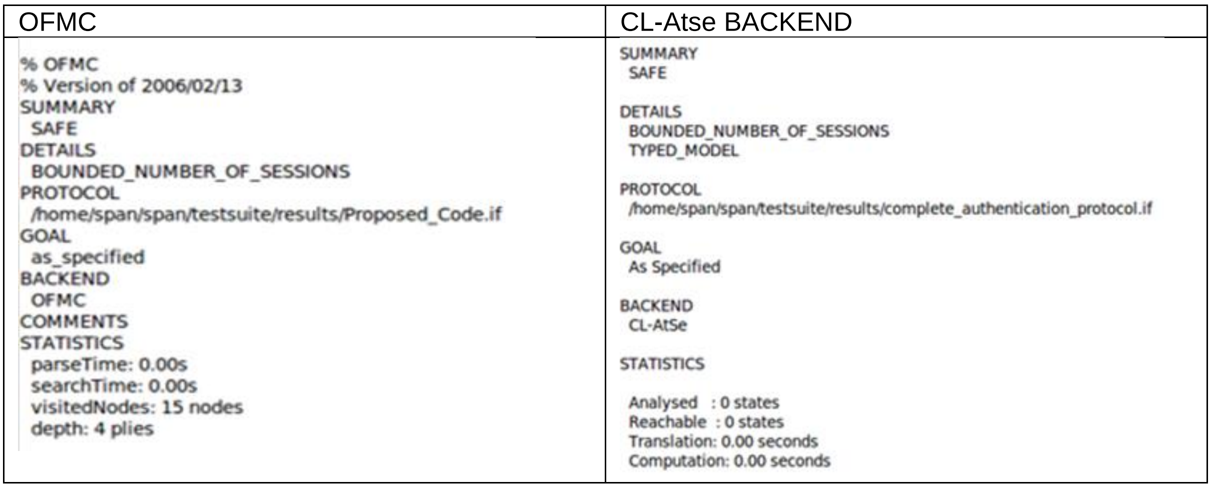
1. A→B:M1=register_request
2. B→A:M2=register_response
3. A→B:M3=start
4. B→A:M4=SessionID
5. A→B:M5=h (R_A ‖N_A)

R_A: 64-bit random number generated by IoT Device A

N_A: Nonce generated by A

6. B→A:M6=confirmation
7. Failure Case: B→A:M7=terminate_sessionB.
8. Session Key Generation: Sk=h(NonceA$\oplus$NonceB) Sk

The protocol begins with the registration phase, where the IoT Device (A) sends a register_request message (M1) to the E-Health Server (B). This step establishes the intent of A to join the system. Upon receiving this request, the server responds with a register_response message (M2), confirming the acknowledgment and preparing for secure communication. This ensures that A is a legitimate participant and allows the protocol to proceed to the next phase. In the session initialization phase, A sends a start message (M3) to B, signalling its readiness to initiate secure communication. The server then generates a unique 64-bit Session ID **(**SID**)** and sends it to A as M4. This Session ID ensures that the communication is uniquely identified and isolated from other sessions, providing a foundation for secure interactions. Next, in the dynamic key exchange phase, A generates a Dynamic Key using a 64-bit random number (R_A) and a nonce (N_A). This key is computed as h(R_A‖N_A) where ‖ represents concatenation. A then sends the Dynamic Key (M5) to B. Upon receiving M5, B validates it. If the validation is successful, B sends a confirmation message (M6) to A, signalling that the exchange is complete and secure communication can proceed. In the failure or attack detection phase, if B detects any anomalies, such as an invalid key or tampered message, it immediately terminates the session by sending a terminate_sessionB message (M7) to A. This mechanism prevents unauthorized access and protects the system from malicious attacks. Finally, in the session key generation phase, both A and B compute a unique Session Key (Sk) for encrypting the communication during the session. The key is derived as Sk=h(NA$\oplus$NB), where $\oplus$ represents the XOR operation between the nonces generated by A and B. This session key ensures that all subsequent data exchanges are secure and protected against attacks such as replay or eavesdropping.



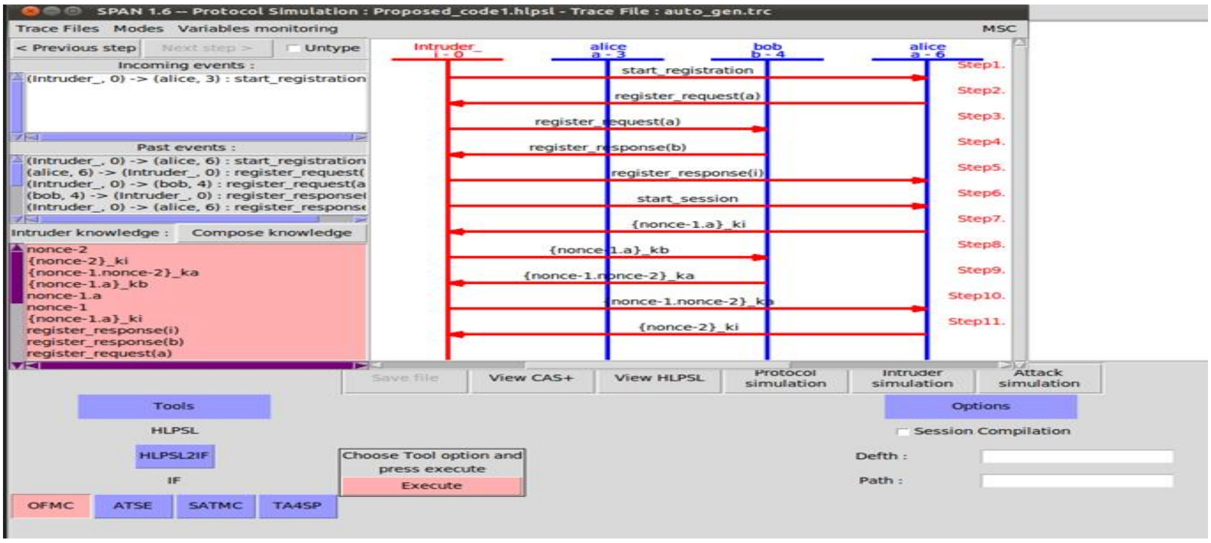
OFMC

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/Proposed_Code.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.00s
  visitedNodes: 15 nodes
  depth: 4 plies
```

CL-Atse BACKEND

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/complete_authentication_protocol.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 0 states
  Reachable  : 0 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds
```

Figure 7: Result Analysis



SPAN 1.6 -- Protocol Simulation : Proposed_code1.hlpsl - Trace File : auto_gen.trc

Incoming events :

(Intruder_, 0) -> (alice, 3) : start_registration

Past events :

(Intruder_, 0) -> (alice, 6) : start_registration
(alice, 6) -> (Intruder_, 0) : register_request(
(Intruder_, 0) -> (bob, 4) : register_request(a
(bob, 4) -> (Intruder_, 0) : register_responsei
(Intruder_, 0) -> (alice, 6) : register_response

Intruder knowledge :

nonce-2
{nonce-2}_ki
{nonce-1.nonce-2}_ka
{nonce-1.a}_kb
nonce-1.a
nonce-1
{nonce-1.a}_ki
register_response(i)
register_response(b)
register_request(a)

Figure 8: Attack Simulation

This image shows attack simulation tool in Avisa(span) where it shows registration process (request and response) and also session start after getting acknowledgment between nodes and authentication process done. It takes 11 steps for communication establishment between nodes.

Justification of Proposed System

The proposed protocol improves on traditional authentication methods by incorporating dynamic key generation, unique session identifiers, and attack detection mechanisms. Unlike static keys or one-sided authentication, which are vulnerable to key compromise, this protocol isolates sessions with different IDs and immediately halts communication if any abnormalities or invalid keys are detected. These features make the system more resilient, secure, and adaptable to emerging threats, providing a more robust solution for IoT environments. The protocol uses cryptographic hashing (h) and XOR operations to secure key exchanges and ensure message integrity. Messages between the IoT device and the server are encrypted using dynamic session keys, preventing intercepted data from being readable. Mutual authentication ensures that both the IoT device and the server authenticate each other before establishing a session, protecting against attackers trying to intercept or manipulate the communication.

Prevention against MITM Attack

To prevent MITM attacks, all communications are encrypted using cryptographic hashes and verified at both ends. The **Session Key (Sk)** is generated independently by both parties as:

$Sk=h(NA \oplus NB)$

- NA = Nonce generated by the IoT device
- NB = Nonce generated by the server
- $\oplus$ = XOR operation

Even if an attacker intercepts M5 or M6, the dynamic session key is not exposed because NA and NB are never transmitted in plain text. Additionally, mutual authentication ensures the IoT Device (A) and Server (B) validate each other's identities using the following exchanges:

1. $A \rightarrow B: M5=h(RA \| NA)$
2. $B \rightarrow A: M6=confirmation$

Prevention Against Replay Attack

The proposed protocol effectively prevents replay attacks by incorporating nonces (NA, NB) and dynamic session keys. Each session utilizes unique random values and nonces to ensure that every authentication process is fresh and time-bound. Even if an attacker intercepts messages from a previous session, these messages cannot be reused because the server verifies the nonces and the dynamic key's validity. This approach ensures that stale or duplicated messages are invalidated, rendering replay attempts futile. The proposed protocol leverages nonces (NA and NB) and cryptographic operations to counter replay attacks. The Dynamic Key (M5) is computed as:

$M5=h(RA \| NA)$

Here, RA is a random 64-bit number, and NA is a nonce. The server verifies M5 and ensures that the nonces and random numbers are unique for each session. Replay attacks fail because any reused M5 would not match the current session's nonce or random number. For example, even if an attacker intercepts:

$M5_{old}=h\ (R_{Aold}||N_{Aold})$

It becomes invalid when the server expects:

$M5_{new}=h(RA_{new}||NA_{new})$

This strict validation ensures freshness and invalidates any previously intercepted messages, rendering replay attempts ineffective.

Communication and Computational Cost Analysis

The results showcase the implementation of an IoT authentication protocol designed to resist common attacks while ensuring efficient communication and computational performance. During the registration phase, each IoT user is assigned a unique session ID by the server, ensuring the legitimacy of users. This phase is lightweight, with the IoT device incurring a computational cost of 11 bytes and the server 10 bytes, resulting in a total registration cost of 21 bytes**.** The authentication process involves secure exchanges between the IoT device and the server, verifying session IDs and dynamic keys to authenticate users. The protocol was tested under several attack scenarios, demonstrating its robustness. In the case of a replay attack, User1 successfully authenticated using a valid dynamic key. This confirms the protocol's ability to prevent unauthorized access by verifying both session IDs and dynamic keys. Similarly, the protocol thwarted an impersonation attack by rejecting authentication for a non-existent user, effectively blocking unauthorized access attempts. A Man-in-the-Middle (MITM) attack was also prevented, with authentication for User2 failing due to a session ID mismatch, further proving the protocol's resistance to data tampering. The protocol maintains cost efficiency with a communication cost of 5 messages and lightweight computational requirements, including 24 bytes for IoT devices and 20 bytes for the server. This ensures suitability for resource-constrained IoT environments. The protocol excels in replay attack protection by verifying session IDs and dynamic keys, MITM attack resistance by detecting data tampering, and impersonation prevention through cross-verification of user credential. So, total cost for Authentication Phase=21 bytes+20 bytes+24 bytes=65 bytes.

Communication cost comparison

Reference	**Registration Phase**	**Authentication Phase**
Tu et al.(Ahmed,2019)	98 bytes	230 bytes
Wu et al.(Ahmed,2019)	102 bytes	238 bytes
Proposed System	32 bytes	80 bytes

Table 2: Communication Cost Analysis

The proposed authentication system enhances efficiency, security, and is well-suited for resource-constrained IoT environments. It reduces computation and communication overhead, requiring only 32 bytes for IoT device registration and 80 bytes for authentication, with a total of just 5 messages exchanged. The protocol uses lightweight operations like XOR and hash functions, making it computationally inexpensive compared to traditional systems that rely on heavy cryptographic algorithms like RSA or ECC. This approach ensures energy and bandwidth efficiency, crucial for IoT devices with limited resources. Security is a key focus, with the system designed to resist common IoT cyberattacks. It prevents replay attacks using dynamic session-specific keys and session ID validation, blocking adversaries from reusing intercepted data. MITM attacks are thwarted by verifying session IDs and keys, while impersonation is prevented through cross-checking credentials with the server registry. The system can detect and end attacks pre-emptively, for example, halting communication when a session ID mismatch is detected. Additionally, the unique session key generation method ensures that even if one key is compromised, other sessions remain unaffected.

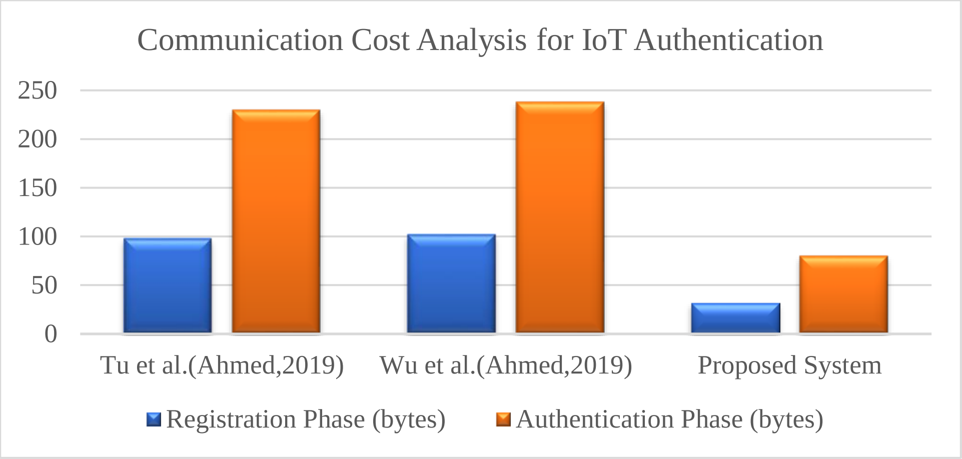


Figure 9: Communication Cost Analysis

Conclusion

The proposed dynamic key-based mutual authentication protocol improves upon existing systems by offering better security and performance, particularly for resource-constrained IoT environments. It protects against replay, MITM, and impersonation attacks using dynamic session keys, nonce-based validation, and lightweight cryptographic operations (XOR and hashing). With a low communication cost of 32 bytes for registration and 80 bytes for authentication, it requires only 5 message exchanges, making it highly efficient for IoT devices. This protocol enables secure mutual authentication between IoT devices and E-Health servers, ensuring the protection of sensitive data and actively detecting and terminating malicious activities. Proven through AVISPA, the protocol is robust against attacks and suitable for critical applications in domains like E-Health. In future work, the integration of ECC and RSA-based hybrid approaches will further enhance the system's security and reliability.

Reference

[1] Wei Emma Zhang, Quan Z. Sheng et al. “The 10 Research Topics in the Internet of Things” *published in 2nd IEEE International conference on RTEICT, 2020*

[2] Amit Kumar Tyagi and Ajith Abraham “Internet of Things: Future Challenging Issues and Possible Research Directions*” published in International Journal of Computer Information Systems and Industrial Management Applications, Vol. 12, pp. 113-124, 2020.*

[3] H. Shin, H. K. Lee, H. Cha, S. W. Heo and H. Kim, "IoT Security Issues and Light Weight Block Cipher," 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2019, pp. 381-384, doi: 10.1109/ICAIIC.2019.8669029.

[4] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[5] Rekha, Shashi & Lingala, Thirupathi & Renikunta, Srikanth & Gangula, Rekha. (2021). Study of security issues and solutions in Internet of Things (IoT). Materials Today: Proceedings. 10.1016/j.matpr.2021.07.295.

[6] Jyoti Neeli, Shamshekhar Patil “Insight to security paradigm , research trend & statistics in internet of things(IoT)” Global Transitions Proceedings, Volume 2, Issue 1, 2021, Pages 84-90, https://doi.org/10.1016/j.gltp.2021.01.012.

[7] C. -I. Zhong, Z. Zhu and R. -G. Huang, "Study on the IOT Architecture and Access Technology," 2017 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES), 2017, pp. 113-116, doi: 10.1109/DCABES.2017.32.

8] Vangelis Gazis, Manuel Goertz Liang et al. “IoT Challenges, Projects, Architectures” *presented at IEEE 18th International Conference on Intelligence in next generation networks , 2015.*

[9] Jean Pierre Nzabahimana “Analysis of Security and Privacy Challenges in Internet of Things” *presented at IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT’2018*

[10] M. Ghahramani, R. Javidan, M. Shojafar, R. Taheri, M. Alazab, and R. Tafazolli, “Rss: An energy-efficient approach for securing iot service protocols against the dos attack,” IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3619–3635, 2021.

[11] M. Stute, P. Agarwal, A. Kumar, A. Asadi, and M. Hollick, “Lidor: A lightweight dos-resilient communication protocol for safety-critical iot systems,” IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6802–6816, 2020.

[12] C. Lyu, X. Zhang, Z. Liu, and C.-H. Chi, "Selective authentication based geographic opportunistic routing in wireless sensor networks for internet of things against dos attacks," IEEE Access, vol. 7, pp. 31068–31082, 2019.

[13] C. Pu, "Sybil attack in rpl-based internet of things: Analysis and defenses," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 4937 4949, 2020.

[14] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing sdn infrastructure of iot–fog networks from mitm attacks," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1156–1164, 2017.

[15] K. Prathapchandran and T. Janani, "A trust aware security mechanism to detect sinkhole attack in rpl-based iot environment using random forest rftrust," Computer Networks, vol. 198, p. 108413, 2021.

[16] N. Pavlovi´ c, M. ˇ Sarac, S. Adamovi´c, M. Saraˇcevi´c, K. Ahmad, N. Maˇcek, and D. K. Sharma, "An approach to adding simple interface as security gateway architecture for iot device," Multimedia Tools and Applications, pp. 1–16, 2021.

[17] B. Maram, J. Gnanasekar, G. Manogaran, and M. Balaanand, "Intelligent security algorithm for unicode data privacy and security in iot," Service Oriented Computing and Applications, vol. 13, no. 1, pp. 3–15, 2019.

[18] M. Hossain and J. Xie, "Third eye: Context-aware detection for hidden terminal emulation attacks in cognitive radio-enabled iot networks," IEEE Transactions on Cognitive Communications and Networking, vol. 6, no. 1, pp. 214–228, 2020.

[19] S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan, and Q. Cao, "Multistage signaling game-based optimal detection strategies for suppressing mal ware diffusion in fog-cloud-based iot networks," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1043–1054, 2018.

[20] M. R. Dey, U. Satapathy, P. Bhanse, B. K. Mohanta, and D. Jena, "Magtrack: Detecting road surface condition using smartphone sensors and machine learning," in TENCON 2019- 2019 IEEE Region 10 Conference (TENCON), 2019, pp. 2485–2489.

[21] Z. Liu and Y. Wu, "An index-based provenance compression scheme for identifying malicious nodes in multihop iot network," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4061–4071, 2020.

[22] A. Agiollo, M. Conti, P. Kaliyar, T.-N. Lin, and L. Pajola, "Detonar: Detection of routing attacks in rpl-based iot," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1178–1190, 2021.

[23] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, "Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles," IEEE Access, vol. 8, pp. 199618 199628, 2020.

[24] C. Marche and M. Nitti, "Trust-related attacks and their detection: A trust management model for the social iot," IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3297–3308, 2021.

[25] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," IEEE Transactions on Sustainable Computing, vol. 4, no. 1, pp. 88–95, 2019.

[26] M. D. Alshehri and F. K. Hussain, "A fuzzy security protocol for trust management in the internet of things (fuzzy-iot)," Computing, vol. 101, no. 7, pp. 791–818, 2019.

[27] S. T. Mehedi, A. A. M. Shamim, and M. B. A. Miah, "Blockchain-based security management of iot infrastructure with ethereum transactions," Iran Journal of Computer Science, vol. 2, no. 3, pp. 189–195, 2019.