EFFICIENT FRAMEWORK OF SECURITY FOR INTERNET OF THINGS

Dr. Mihir Mehta[1], Dr. Kajal Patel[2], Dr. Komal Anadkat[3]

•

[1]Assistant Professor, Computer Engineering department, G.E.C., Gandhinagar, Gandhinagar, India. mihir_mehta@gecg28.ac.in

[2] Associate Professor, Computer Engineering department, Vishwakarma College of Engineering, Ahmedabad, India. kajalpatel@vgecg.ac.in

[3]Assistant Professor, Information Technology department, G.E.C., Gandhinagar, Gandhinagar, India. komalanadkat@gecg28.ac.in

Abstract

IoT security represents a highly compelling subject of research at present. The absence of a viable security solution for IoT applications could render them ineffective across various domains such as healthcare, smart homes, inventory management, smart agriculture, and more. Within the IoT architecture, security services like Confidentiality, Integrity, and Authentication play pivotal roles. In our research, we have concentrated on the Authentication service, which is fundamental for distinguishing users and devices unequivocally within a network. Authentication serves as the initial and crucial step in establishing secure communications among diverse IoT devices and users within the network. A compromised Authentication service could open the door for unauthorized users or devices to infiltrate the network, potentially leading to harmful activities like Masquerade attacks, Man-in-the-Middle (MITM) attacks, and Replay attacks.Currently, Authentication stands as a widely adopted and essential method for granting access to devices within IoT networks. Our contribution involves the development of a Multi-factor IoT Authentication Model, leveraging two key parameters: Device Context Information and Dynamic Key-based authentication.Our proposed approach begins by verifying the origin of information. If the origin is deemed valid, our model proceeds to validate the identity of the device. In the event of an intruder attempting to manipulate the device's origin from its predefined context to an alternative location, our system can swiftly detect this deviation, thereby enabling the rejection of communication requests from compromised devices.Following the verification of context information, we initiate mutual authentication between the IoT device and the server, employing the Challenge-response model. As a result of this second step, individual Session keys are generated at both the device and server sides, facilitating secure communication within a specific time window.

Keywords: Internet of Things, Multi-factor Authentication, Dynamic key based Authentication.

I. Introduction

The realm of IoT security represents a highly significant area of research in the current era. It has garnered substantial attention from researchers across industry, academia, and various government agencies. A report by CISCO in April 2019 projected a staggering 50 billion devices to be interconnected with the internet by the end of 2020. This exponential growth presents a substantial opportunity for malicious actors to launch diverse cyber-attacks on IoT systems, primarily due to the open architecture inherent in IoT networks. Traditional security approaches are ill-suited for IoT devices, primarily due to their inherent limitations, including constrained storage capacity and computational power. Moreover, IoT devices must function in harsh and unpredictable environments, making them vulnerable to an array of security threats. Consequently, there is an

imperative need to develop security solutions tailored to the resource constraints of IoT devices while providing essential attributes such as Confidentiality, Integrity, and Authentication in IoT networks.

Outlined below are some of the key challenges in IoT security.

Open Architecture: In IoT, all devices are interconnected through the internet, adhering to an open framework. This openness amplifies the potential for various security threats.

System Limitations: IoT devices face constraints concerning memory, computational power, CPU capacity, and energy. These limitations render traditional security approaches unsuitable for direct deployment in IoT systems.

Absence of Standards: The diversity of IoT devices hinders standardization efforts. Each IoT device functions as a standalone system comprising hardware, firmware, and communication interfaces. Ensuring security at the design phase, crafting secure code, and conducting rigorous verification/validation during the manufacturing process are essential. Nevertheless, there is currently no practical means to enforce and standardize these security methods across all devices.

Deficient Trust and Integrity: With a multitude of devices connected to the internet, it becomes nearly impossible to verify that each device maintains adequate safeguards and remains up-to-date with the latest security updates. A single vulnerable link in the network can grant intruders access to numerous devices. Ensuring trust and data integrity for every IoT device is of paramount importance.

Insecure Web Interfaces: Vulnerable web interfaces in IoT devices are susceptible to various threats, including account enumeration and brute force attacks. For example, attackers may gain unauthorized access to websites by attempting numerous password combinations, potentially compromising administrative policies and sensitive data. Attackers can also manipulate the credentials of legitimate users.

Addressing these challenges is crucial to establishing a robust and secure IoT ecosystem that can withstand the evolving landscape of cyber threats.

There are certain security issues present in IoT Architecture, they are Authentication, Encryption, Trust Management & Secure Routing.

Authentication: Authentication plays a pivotal role in identifying devices and users within an IoT system, granting access exclusively to authorized entities. In IoT systems, authentication can be realized through various methods, including Identity-based authentication, Token-based authentication, PUF-based authentication, and Procedure-based authentication.

Encryption: Encryption is essential for achieving end-to-end security in IoT systems. The primary objective of encryption within the IoT ecosystem is to establish effective end-to-end communication through the utilization of symmetric and asymmetric cryptographic algorithms. However, IoT devices face resource limitations, which necessitate a departure from traditional encryption algorithms like AES and DES, as they are not directly suitable for the constraints of IoT networks.

Trust Management: IoT trust management is fundamentally geared towards identifying and isolating malicious nodes within the IoT network. The overarching aim is to identify and subsequently remove such nodes from the network, thus enabling secure access control within the IoT environment.

Secure Routing: Within the context of data transmission in IoT networks, the presence of malicious nodes poses a significant threat. These malicious nodes have the potential to divert data packets towards them, infiltrating routing and forwarding decision processes for both data and control packets. As such, ensuring secure routing mechanisms becomes imperative in safeguarding the integrity of IoT networks.

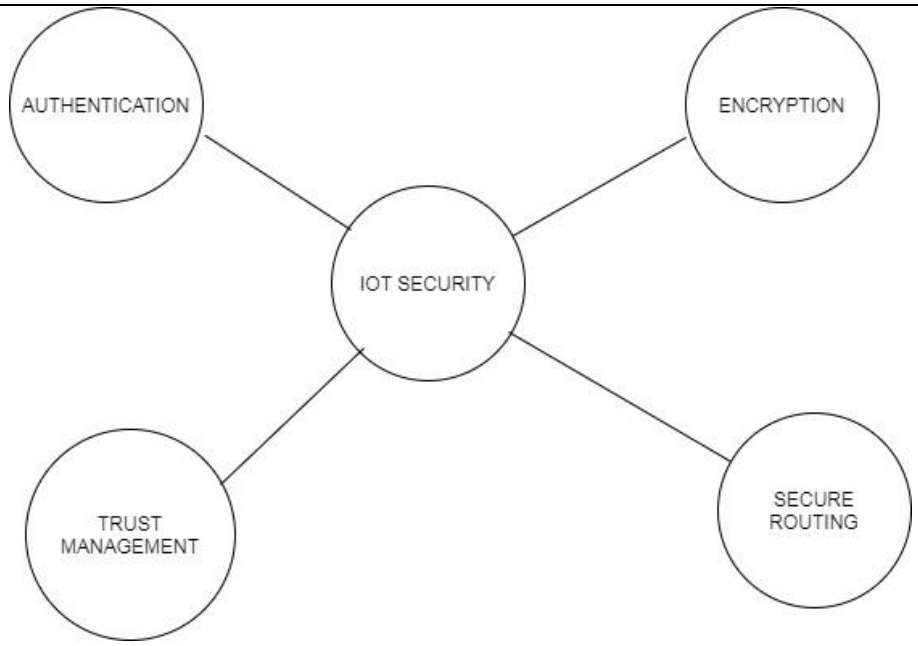

Figure 1: *Security Issues for Internet of Things*

II. Literature Review

In [1], researchers Hokeun Kim and Edward Lee proposed an approach for authentication in IoT devices, emphasizing a provincially centralized and universally distributed method. Trust serves as a fundamental prerequisite for authentication in IoT systems, and the authors discussed the implementation of a certificate-based scenario to establish trust between clients and servers. They identified two key methods for deploying trust within a network: (1) Utilizing a Centralized Trusted Authority and (2) Leveraging Distributed and Trusted stakeholders. The authors developed a network framework named "Auth," which incorporates local authentication and authorization entities. Auth, implemented as open-source software in Java and accessible on GitHub, facilitates authorization for locally registered entities (IoT devices) and manages trust relationships with other Auth instances. The framework securely stores the credentials of endorsed devices and access policies within a database. The authorization process involves the assignment of session keys, cryptographic keys used for specific access activities.

In [2], authors Mohammad Wazid, Ashok Kumar Das, and others discussed a lightweight authentication protocol known as the "User Authenticated Key Management Protocol (UAKMP)" designed for a concept called Hierarchical Internet of Things (HIOT). This protocol utilizes three authentication factors: (1) user smart cards, (2) passwords, and (3) personal biometrics. The method employs a combination of cryptographic message digest functions and symmetric encryption/decryption. UAKMP involves six essential steps: (1) Enrollment of various sensor nodes, (2) Enrollment of users, (3) User sign-up, (4) Authentication and key agreement, (5) Password change, and (6) Integration of newly joined sensor nodes. Gateway nodes store critical information required for authentication in all deployed sensing nodes, including their identity. The protocol assumes that the Gateway node is trustworthy, as a breach of its security could endanger the entire network, potentially leading to node impersonation attacks and denial of service attacks.

In [3], authors Ning Wang, Ting Jiang, and their team presented an authentication approach primarily focused on physical layer attributes. Physical layer authentication involves the examination of various physical attributes, including Received Signal Strength (RSS) and Channel

Impulse Response (CIR). The proposed method incorporates machine learning, specifically a Feedforward Neural Network, for classification tasks. This choice of neural network offers advantages such as rapid learning, ease of construction, and minimal human intervention. Binary hypothesis testing is used to detect spoofing attacks, framing the problem within an Alice-Bob-Eve model, where Alice is the legitimate transmitter, Bob is the legitimate receiver, and Eve is an illegitimate transmitter attempting to impersonate another node with a false address. The challenge addressed in this method is determining whether the second message received by Bob, after the first one confirmed to be from Alice, is still sent by Alice or not.

In [4], authors Muhammad Naveed Aman, Sachin Taneja, and others introduced a token-based authentication method that employs OAuth 2.0, an open authentication and authorization standard. This method aims to mitigate security risks associated with conventional client-server authentication, where clients use resource owners' credentials, potentially leading to password leakage and data breaches. The proposed approach involves three main steps: (1) The client sends an authorization request to the Authorization Server (AS), (2) The AS verifies the client's authenticity and, if verified, issues an access token to the client, and (3) The client uses this access token to authenticate itself to the resource server (RS) and access requested resources. However, the method is susceptible to replay attacks if an intruder captures an access token generated by the Authorization Server, as it could be misused for impersonation attacks.

In [5], authors Prosanta Gope and Biplab Sikdar presented a lightweight two-factor authentication approach for IoT devices, addressing the vulnerabilities of password-based and key-based methods to physical and side-channel attacks. Their approach combines two factors: (1) a secret shared key and (2) a Physical Unclonable Function (PUF). During registration, an IoT device transmits its identity along with a registration request to the server. The server responds by generating a random challenge (C), which it sends back to the client IoT device. The client computes a response to the challenge using its PUF and sends it back to the server for verification. If the response is correct, the server generates an alias identity and session key for the device, storing these details in its database. However, the method does not consider environmental parameters, which can affect PUF output, and is vulnerable to man-in-the-middle attacks, replay attacks, and spoofing attacks.

In [6], authors Muhammad Naveed Aman and Biplab Sikdar presented two-factor authentication algorithms for IoT devices, considering the low-cost nature of IoT devices that makes them susceptible to spoofing and impersonation attacks. Their method combines PUF and device hardware fingerprints for authentication. After device identity verification, the server provides a new challenge to the IoT device, which computes a response using its PUF and the provided challenge. However, this approach is vulnerable to replay attacks, as intruders can intercept Challenge-Response pairs exchanged between the IoT device and the server and use them for predicting other CRPs. Additionally, it does not provide security against man-in-the-middle attacks.

In [7], authors Zahoor Ahmed Alizai, Noquia Fateema Tarin, and others introduced a multifactor authentication approach based on digital signatures and device capabilities. This schema utilizes a secure TLS channel, with a digital signature serving as a second factor for authentication. Device authentication relies on the verification of device capability, involving data processing tasks. However, this approach demands high computational resources due to the involvement of asymmetric cryptography, making it unsuitable for resource-constrained IoT devices. Furthermore, it is vulnerable to impersonation and denial-of-service attacks.

In [8], authors Moritz Loske, Lukas Rothe, and others proposed context-aware authentication methods for IoT devices, addressing the limitations of existing cryptography-based approaches in IoT networks with resource-constrained devices. Context-aware authentication incorporates environmental information, such as temperature, luminosity, radio signals, and device location, to improve the authentication process. While this method reduces computational overhead, it does not provide confidentiality and is susceptible to man-in-the-middle attacks, replay attacks, and spoofing attacks. Therefore, it is best used as one parameter within a multi-factor-based authentication approach to enhance security.

In [9], authors Tarak Nandy, Sananda Bhattacharya, and their team discussed the existing authentication approaches for IoT and emphasized the need for strong and secure authentication methods. In IoT networks, various devices communicate with each other and users, making proper security crucial to prevent credential theft and attacks on the IoT network. The authors identified various attacks on IoT authentication, including masquerade attacks, man-in-the-middle attacks, denial-of-service attacks, forging attacks, guessing attacks, physical attacks, and routing attacks.

Table 1: *IoT Attacks & description*

Attacks	Description
Masquerade attack	In this attack, adversary misuses the identity of the legal user to get access to the network.
Man in the Middle attack	In this attack, adversary intercepts the communication between two parties and also can modify the communication contents.
DOS attack	In this attack, adversary floods the network with fake requests so legal user cannot use resources at that time. Network and resources are unavailable for them.
Forging attack	In this attack, adversary emulates a system or legal user to gain access to the network.
Guessing attack	In this attack, adversary predicates credentials of legal user by brute force approach or dictionary approach to gain access of the network.
Physical attack	In this attack, adversary tries to get physical access of the resource and can change physical location of resource to launch the attack.
Routing attack	In this attack, adversary advertises a false route for packet delivery from source to destination.

Problem Statement: Design & Development of Lightweight Multi-factor IoT Authentication approach by considering Context Parameter & Dynamic Key Parameter (Vault, Random Number) for addressing location spoofing attack, Eavesdropping attack, Replay attack & Identity Stolen attack.

Advantages of Context Information Parameter:

Early Detection of Attackers: When contextual variables, such as location information, are validated during the login session, it becomes possible to identify and detect request messages from potential attackers at an early stage. This early detection eliminates the need to unnecessarily verify other authentication factors during the session, thereby enhancing the security system's performance and reducing delays.

Crucial for Decision-Making: In domains like Military and Industry applications, the context parameter of a device plays a pivotal role in the decision-making process. If a device is legitimate but its context information has been tampered with, it can transmit incorrect or faulty data, which can have adverse effects on system performance. Therefore, validating context information is essential, along with device identity validation, before initiating a communication session.

Advantages of Dynamic Key-Based IoT Authentication:

Enhanced Security: In symmetric encryption, both communicating parties share the same pair of keys. However, if a third party gains access to the key or analyzes network traffic, they can infer the communication content. Consequently, long-term use of a fixed session key is insecure in IoT devices.

"One Time One Cipher" Approach: To address this security concern, the "One Time One Cipher" approach is employed, where the key used for encryption and decryption differs for each session

and expires after each use. This approach ensures the uniqueness and dynamic nature of the key. Session keys are generated securely and efficiently on both the device and server sides, considering parameters such as the Vault and Random Number Generation. This proactive measure helps prevent Key Stolen and Eavesdropping attacks, enhancing overall security.

III. Methodology

Step 1: Context-Based Authentication

A. During the login request to the server, an IoT device transmits its login request along with contextual information. Specifically, the IoT device sends its location information in the form of Cartesian coordinates to the server.

B. The server proceeds to validate these context parameters by comparing them to the stored records in its database. In this validation process, the server calculates the Angle of Arrival (AoA) for the requested IoT device and matches the result with the stored AoA information for that device in the database. If these physical context parameters match, it provides evidence that the device is legitimate and identified at its original location.

Step 2: Dynamic Key-Based Authentication

If the device successfully passes the context-based authentication test, we introduce a second factor to enhance our authentication process, known as Dynamic Key-Based Authentication. In this phase, IoT Device and Server mutually authenticate each other initially by employing a Challenge-Response mechanism.Following a successful mutual authentication, a Session Key is generated for communication within a specific time window.

The detailed procedure for Dynamic Key-Based Authentication is as follows:

Vault: The Vault consists of 64 keys, with each key being 128 bits in length and represented in hexadecimal format. All of these keys are organized in an 8x8 matrix format, which is stored both on the IoT device and the server. To enhance security, these keys can be stored in an encrypted format at both ends. Each key in this 8x8 matrix can be denoted as K[0][0], K[0][1], …, K[7][7]. During the initial deployment, this 8x8 matrix is shared between the IoT device and the server.

Challenge-Response Mechanism: Our proposed protocol employs a Handshaking concept to achieve mutual authentication between the IoT device and the server. The diagram below illustrates the sequence of messages exchanged between the IoT device and the server to facilitate Mutual Authentication.

Table 2: *Notations for the proposed Dynamic Key Based Authentication*

Notation	Description
||	Concentation Operation
⊕	Ex-OR Operation
h	Message Digest Function
Random Number	128-bit Random Number for Mutually Authentication Purpose
Temporary Number (Nonce)	128-bit Random Number for Session Key Generation Purpose

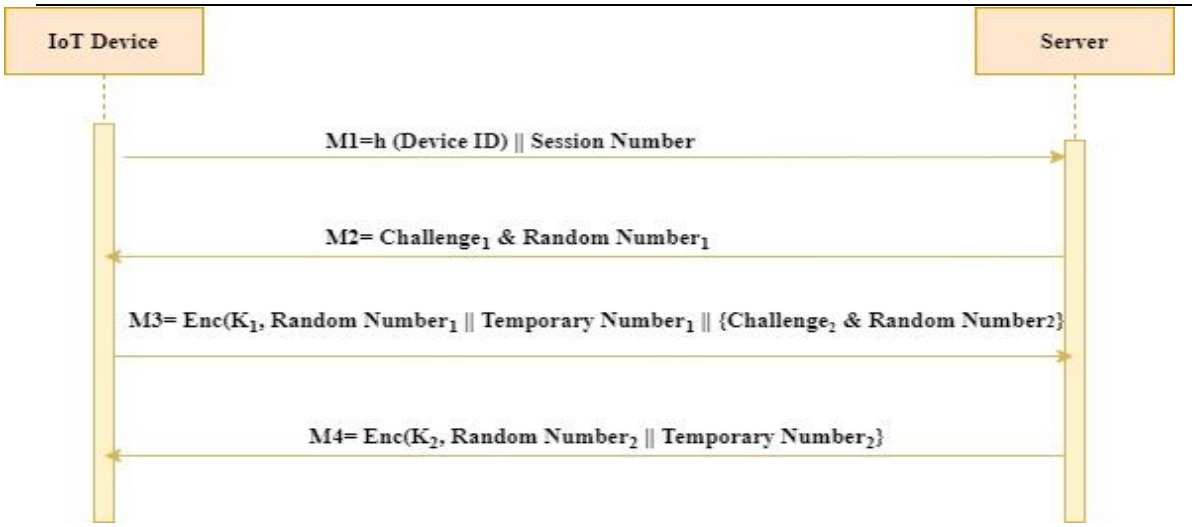

Figure 2: *Message Exchange Sequence for the proposed authentication structure*

The communication process between an IoT Device and an IoT Server involves several steps to establish a secure authentication session. Below is a description of these steps.

1. **Initiation of Communication Request:**
   - The IoT Device initiates communication by sending a request (M1) to the IoT Server.
   - Request message M1 includes a message digest of the Device ID and the Session number, which helps maintain the authentication session.
   - M1 = h(Device ID) || Session Number
2. **Challenge Message Generation by Server:**
   - The Server verifies the message digest value for the Device ID.
   - If valid, the Server generates a Challenge Message (M2) for the IoT Device.
   - M2 contains Challenge1 and a Random number1.
   - Challenge1 comprises q distinct numbers, each pointing to an index in an 8x8 Matrix stored in a secure vault.
   - The value of q must be less than the total number of keys stored in the vault.
   - Challenge1 = {C1, C2, C3, … , C8}
   - M2 = {Challenge1, Random Number1}
3. **Response Generation by IoT Device:**
   - The IoT Device generates a response for the assigned challenge.
   - A temporary key of 128 bits (K1) is generated by performing XOR operations on the key values indexed by the challenge message.
   - Temporary Key K1 at IoT Device Side = K[C1] ⊕ K[C2] ⊕ … ⊕ K[Cq]
   - The IoT Device creates a response by encrypting Random Number1 || Temporary Number1 using K1 as the encryption key.
   - Here, Temporary Number1 is a 128-bit random number generated by the IoT Device for future use in generating a Session key for subsequent communication.
   - M3 = Enc(K1, Random Number1 || Temporary Number (Nonce)1 || {Challenge2 , Random Number2}).
   - The IoT Device also generates a separate challenge message (Challenge2) for the IoT Server in a similar manner.
4. **Response Generation by Server:**
   - Upon receiving the message from the IoT Device, the Server generates a temporary key (K2) using the indexes from Challenge2 stored in its secure vault.
   - No key sharing is required between the IoT Device and the Server.
   - After obtaining key K2, the Server decrypts message M3.

- If the Server retrieves Random number1 from M3, it indicates that the receiver of the previous challenge message (M2) was a legitimate IoT Device.
- The Server then generates a response for the IoT Device's challenge (M3).
- Message M4 from the Server to the IoT Device is encrypted using temporary key K2 and includes Random Number2 and Temporary Number2.
- Temporary Key K2 at Server Side = K[C1] ⊕ K[C2] ⊕ … ⊕ K[Cq].
- M4 = Enc(K2, Random Number2 || Temporary Number (Nonce)2).

5. **Authentication by IoT Device:**
   - The IoT Device receives message M4 and decrypts it by generating temporary key K2 from its secure vault, using the content of Challenge C2.
   - If the IoT Device obtains Random number2, it signifies that the Server is also authenticated.
6. **Session Key Generation:**
   - After mutual authentication between the IoT Device and the Server, they generate a temporary session key using Temporary Number1 and Temporary Number2.
   - Session Key = Temporary Number1 ⊕ Temporary Number2.

Contribution of our Research Work:

1. The proposed work aims to implement light weight mutual authentication approach for IoT devices which can avoid the possibility of Key Stolen attack, Eavesdropping attack and Location Spoofing attack.
2. The proposed work plans to verify contextual information of a device when it initiates a session with reference node. Parameter AoA- Angle of arrival will be utilized for context matching. So, prevention of Location Spoofing attack can be done at initial stage. It will reduce energy consumption, delay and also intrusion activities during session.
3. The proposed work plan to generate the session key as a part of IoT device authentication in a dynamic way. The working principal for dynamic key generation will be "One Session, One Cipher". It will generate session key on both sides –device and server in a secure, efficient way by considering parameters- Vault and Random number generation. So, prevention of Key Stolen attack and Eavesdropping attack will be possible.

IV. Security Analysis of the Proposed Method

Protection against Location Spoofing Attack:

Proof: The distinguishing feature of the proposed protocol lies in its ability to verify the location of the IoT device, ensuring that authentication requests originate from a known location. Consequently, if an adversary seizes an IoT device and attempts authentication from a remote, unauthorized location, their efforts will be in vain. We have implemented a Localization approach, utilizing location-specific attributes such as AoA (Angle of Arrival), to fortify protection against Location Spoofing attacks.

Protection against Man-in-the-Middle Attack:

Proof: A Man-in-the-Middle (MitM) attack involves an attacker intercepting communications between two parties with the intention of secretly eavesdropping on or modifying the transmitted data. The significant feature of the proposed method is that adversaries cannot compute the session key due to the reliance on Random number generation in its generation process. Importantly, in our protocol, the session key is not explicitly transmitted between the Server and the device. Instead, it is computed independently by the device and server at their respective locations. Consequently, adversaries are unable to access the session key required to launch a MITM attack.

Protection against Replay Attack:

Proof: The initiation of a new session with a device encompasses both the context-based authentication process and the dynamic key-based authentication approach for key establishment.

During this authentication phase, each device shares a nonce and a Session ID. The Session ID is unique for each new session and serves as a timestamp within our protocol. In the event of an attacker attempting to replay previous session authentication messages, these messages will be discarded due to the presence of an old Session ID that has already expired. Furthermore, the attacker cannot manipulate or update the Session ID as it is transmitted in an encrypted form, with only the destination node, i.e., the Server, possessing the knowledge of it after decryption with its key. Even if an adversary were to submit the same authentication message to the server after a certain period of time, they would not succeed. This is because our protocol generates a new Nonce (Random Number) for each session, rendering any previous nonce random number request for session establishment immediately invalid.

Device Anonymity:

Proof: In relation to Device Anonymity, our proposed approach refrains from transmitting the actual device identity in any message exchange or communication with the server node. Instead of the device ID, a message digest value of the device ID is transmitted along with the session number. Since the message digest function adheres to a one-way property, it becomes computationally infeasible for an intruder to deduce the device ID from the message without knowledge of the specific hash algorithm used.

Brute force attempts Analysis for the proposed Approach:

We have securely stored a total of 64 keys, each with a length of 128 bits, in both the IoT device and the Server's vaults. Temporary keys are generated through the XOR operation using these stored keys. Let's calculate the efforts required to derive these Temporary keys.

An intruder needs to select 8 keys out of the total 64 keys, resulting in a total possible combination of 64C8, calculated as follows:

$^{64}C_8$ = 64! / (64-8)! 8!

= 64! / 56! 8!

= 64*63*62*61*60*59*58*57 / 8*7*6*5*4*3*2*1

= 17, 84, 62, 98, 76, 37, 760 / 40, 3 20

Total Possible key combinations at IoT device side = 4,42,61,65,368.

Similarly, total possible key combinations at Server side for selecting 8 different keys from 64 keys vault to generate second temporary key = 4,42,61,65,368.

Total computations required to capture both temporary key from vault= 8,85,23,30,736.

Assuming that an intruder can perform 1 million computations in 1 hour, it would take them a total of 8,852.33 hours or approximately 368 days to recover Temporary Key 1 and Temporary Key 2 from the vault. This is a significant time frame, and since we also update vault values regularly, our suggested schema provides security against Key-stolen attacks.

Even if an adversary possesses knowledge about the dynamic key authentication approach, it remains computationally infeasible for them to directly derive the session key.

V. Conclusion

The Internet of Things (IoT) encompasses a multitude of physical devices capable of seamless data exchange. These devices connect directly to the web, operating in an open environment, which presents opportunities for intruders to launch various cyber-attacks. IoT security is a critical research domain that engages both academic and industry researchers. Within the realm of IoT security, the CIA Model—Confidentiality, Integrity, and Authentication—is of paramount importance. Authentication, in particular, plays a central role in ensuring the security of IoT networks as it uniquely identifies each device connected to the network. In our investigation, we thoroughly examined the challenges inherent in existing IoT authentication algorithms. We uncovered potential cyber threats, including Replay attacks, Man-in-the-Middle (MITM) attacks, Location Spoofing attacks, and Key Stolen attacks, which can compromise the security of current IoT authentication architectures. Furthermore, we conducted an in-depth review of the work conducted by various

experts in the field of authentication. Through this review, we pinpointed research gaps that still exist in the domain of IoT authentication, highlighting opportunities for researchers to contribute their expertise and develop precise and efficient security solutions. There is a pressing need for the creation of an efficient IoT Authentication Multi-factor algorithm that is lightweight—demanding fewer resources—and is rooted in context verification and dynamic key generation approaches.
To substantiate our proposal, we conducted an informal security analysis, demonstrating that our approach effectively safeguards against Key Stolen, MITM, and Replay threats. Furthermore, we established that it is computationally infeasible for an intruder to breach our suggested approach within a finite timeframe and with limited resources.

References

[1] Hokeun Kim and Edward A. Lee (2017). Authentication and Authorization for the Internet of Things, *IEEE Internet of Things Journal, 19: 27-33.*

[2] Mohammad Wazid, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Mauro Conti, Minho Jo (2017). Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks, *IEEE Internet of Things Journal, 5:269-282*.

[3] Ning Wang, Ting Jiang, ShichaoLv and Liang Xiao, Senior Member (2017). Physical-Layer Authentication Based on Extreme Learning Machine. *IEEE Communications, 21:1557-1560*.

[4] Muhammad Naveed Aman, Sachin Taneja, Biplab Sikdar, Kee Chaing Chua, and Massimo Alioto (2019). Token-Based Security for the Internet of Things With Dynamic Energy-Quality Tradeoff, *IEEE Internet of Things Journal, 6:2843-2859*.

[5] Vikas Hassija, Vinay Chamola ,Vikas Saxena , Divyansh Jain, Pranav Goyal, And Biplab Sikdar (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures, *IEEE Access, 7:82721-82743*.

[6] Prosanta Gope and Biplab Sikdar (2018). Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices, *IEEE Internet of Things Journal, 6:580-589*.

[7] Sulabh Bhattarai and Yong Wang (2018). End-to-End Trust and Security for Internet of Things Applications, *IEEE Computer Society, 51:20-27*.

[8] Muhammad Naveed Aman, Mohamed Haroon Basheer and Biplab Sikdar (2019). Two factor Authentication for IOT with Location Information, *IEEE Internet of Things Journal, 6(2): 3335-3351*.

[9] Yan Zhao, Shimming Li and Liehui Jiang (2018) Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multi-server Environment, *WILEY Hindawai Security and Communication Networks, 18:1-13*.

[10] Majid Alotaibi (2018). An Enhanced Symmetric Cryptosystem and Biometric-Based Anonymous User Authentication and Session Key Establishment Scheme for WSN, *IEEE Access, 6:70072-70087*.

[11] Zahoor Ahmed Alizai, Noquia Fatima Tareen and Iqura Jadoon (2018). Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures, *IEEE International Conference on Applied and Engineering Mathematics, https://doi.org/10.1109/ICAEM.2018.8536261*.

[12] Moritz Loske, Lukas Rothe and Dominik Gertler (2019). Context-Aware Authentication: State-of-the-Art Evaluation and Adaption to the IIoT, *IEEE 5th World Forum on Internet of Things (WF-IoT), https://doi.org/10.1109/WF-IoT.2019.8767327*.

[13] Armin Babaei, Gregor Schiele (2019). Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges, *Sensors, 19 (14):3208 https://doi.org/10.3390/s19143208*.

[14] Baibhab Chatterjee, Shovan Maity (2019) RF-PUF: Enhancing IoT Security through Authentication of Wireless Nodes using In-situ Machine Learning, *IEEE Internet of Things Journal, 6(1): 388-398.*

[15] Tarak Nandy, Norjihan Abdul Ghani and Sananda Bhattacharya (2019). Review on Security of Internet of Things Authentication Mechanism, *IEEE Access, 7: 151054-151089*.

[16] Santosh Krishna B V and Gnanasekaran T (2017). A Systematic Study of Security Issues in Internet-of-Things (IoT), *IEEE International conference on I-SMAC, https://doi.org/10.1109/I-SMAC.2017.8058318*.

[17] Mardiana binti Mohamad Noor, Wan Haslina Hassan (2019). Current research on Internet of Things (IoT) security: A survey, *ELSEVEIR Computer Networks, 148: 283-294*.

[18] Chang-le Zhong, Zhen Zhu and Ren-gen Huang (2017). Study on the IOT Architecture and Access Technology, *IEEE 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, https://doi.org/10.1109/DCABES.2017.32*.

[19] Jeffrey Voas, Bill Agresti (2018). A Closer Look at the IoT's "Things", *IEEE Computer Society, 20 (3): 11-14*.

[20] Jyoti Deogirikar and Amarsinh Vidhate (2017). Security Attacks in IoT: A Survey, *IEEE International conference on I-SMAC, https://doi.org/10.1109/I-SMAC.2017.8058363*.

[21] Zhiping Jiang, Kun Zhao and Junzhao Du (2020). PHYAlert: identity spoofing attack detection and prevention for a wireless edge network, *Journal of Cloud Computing, 9 (5):1-13*.