[1]Gaikwad Vidya Shrimant

[2]K. Ravindranath

[3]Gudapati Syam Prasad

IoT Device-to-Cloud Continuous Authentication using Lightweight Key Establishment Mechanism

Journal of Electrical Systems

Abstract: - Cloud computing is an important component for the success of the Internet of Things (IoT). IoT devices generate massive amounts of data, and cloud computing provides the necessary infrastructure to store, process, and analyze this data. The IoT environment is heterogeneous and connects billions of devices, making it a high-value target for attackers. Impersonation attacks and denial-of-service attacks (DoS) are two common threats that can compromise the availability and security of IoT devices. Continuous authentication is a technique that can help mitigate the risk of session hijacking and unauthorized access to IoT devices. While many existing continuous authentication schemes focus on cloud-to-device authentication, it is also important to authenticate devices themselves, as a compromised device can put the entire system at risk. This research proposes a solution for a secure cloud-to-device continuous authentication protocol that relies on devices' features (such as token, battery). Continuous authentication has been introduced as a solution to the problems related to static authentication. The protocol considers the software and hardware limitations of smart IoT devices by using hash function lightweight cryptography.

I. INTRODUCTION

The use of IoT devices in critical environments, such as medical facilities, government facilities, and financial institutions, raises concerns about privacy and security. While wearable sensors and devices can provide valuable data for monitoring and tracking, they can also potentially be misused by authorized users or hacked by malicious actors.

Overall, the use of IoT devices in critical environments can provide valuable benefits for monitoring and tracking, but it is essential to balance these benefits with privacy and security considerations.

Authentication of IoT devices poses several challenges due to their limited software and hardware capabilities, as well as the heterogeneity of the IoT environment. Some of the key challenges that arise in this context include: Limited computational resources, Connectivity issues, Lack of standardization, Security risks.

To address these challenges, researchers and developers are exploring a range of new authentication techniques specifically tailored to the needs of IoT d[1]evices. Some of these techniques include lightweight cryptographic algorithms, biometric authentication, and decentralized identity systems.

Many of the researcher found the solution of static authentication in which device are verified at the start of every new session. Static authentication is vulnerable to some attacks like hijacking of sessions, since here device is authenticated only once at the start of every session.

Continuous authentication is a security mechanism that verifies the identity of a user or device throughout a session, rather than just at the beginning of the session. This helps prevent unauthorized access and impersonation at any time during the session.

Continuous authentication is particularly useful in situations where a large amount of data is being transmitted between devices over a short period of time. Instead of re-authenticating each time before re-transmission, continuous authentication can be used to speed up the process while still maintaining security.

Some examples of continuous authentication include biometric authentication, such as fingerprint or facial recognition, or behavioral authentication, which analyzes user behavior patterns to verify identity. These methods

[1]Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

Mail id: gaikwad.vidya30@gmail.com

[2]Supervisor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

Mail id: ravindra_ist@kluniversity.in

[3]Supervisor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

Mail id: syamprasad.gudapati@gmail.com

can help ensure that the user or device remains authenticated throughout the session, without requiring constant manual re-authentication. To overcome the drawbacks of static authentication, we introduced continuous authentication.

Continuous authentication is a security method that involves verifying the user's identity on an ongoing basis, even after the initial login. It typically involves the use of a token or some other form of identity verification, which is checked periodically to ensure that the user is still present and authorized to access the system or data. If the token is no longer present, the system may automatically lock or log the user out to prevent unauthorized access.

Static and Continuous Authentication

Table 1: Comparison of static and dynamic authentication

Parameters	Static Authentication	Continuous Authentication
Security Levels	**Less Secure:** Reusing the same information, such as usernames and passwords, across multiple digital systems can be a significant security risk	**More Secure:** Dynamic authentication typically involves the use of one-time passwords (OTPs), which are time-sensitive and can only be used once for authentication.
Ease in Implementation	**Easier:** may not require as much infrastructure compared to dynamic authentication	**Difficult and expensive**: one-time passwords (OTPs) or other time-sensitive credentials are generated, these credentials are typically only valid for a short period of time and are replaced with new ones after each use, which requires the constant generation of new passwords.
Areas Used	Used for low-risk environments, such as personal email accounts	recommended for accounts with a high risk of security attacks, such as those with finances, assets, or enterprise information
Convenience	Less convenient	More convenient
Flexibility	Less flexible: Static authentication typically relies on a single authentication factor, such as a password or a security token, and does not provide the user with the option to choose from multiple authentication methods.	More flexible: dynamic authentication offers more flexibility, customization, and security

Authentication Techniques in IoT

The most commonly used technique is the authentication system based on shared secrets, keys, or passwords. Other techniques include biometric authentication, multi-factor authentication, and continuous authentication. Biometric authentication involves using physical or behavioral characteristics of the user, such as fingerprints or voice recognition, for identity verification. Multi-factor authentication involves using multiple methods of authentication, such as a password and a fingerprint scan. Continuous authentication involves ongoing verification of the user's identity even after logging in, such as through the use of tokens that signal the user's presence.

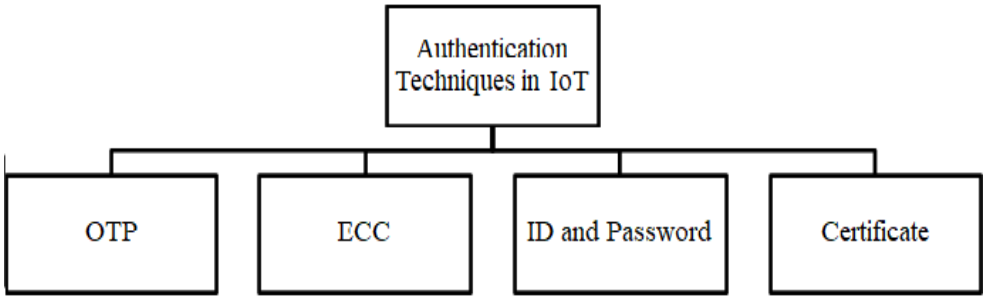

Figure 1: Authentication Techniques in Cloud IoT

1) Authentication with OTP

A one-time password (OTP) is a security feature that is commonly used to authenticate users during the login process. OTPs are temporary passwords that are typically valid for a short period of time and can only be used once.

When a user logs in using an OTP, they are required to enter the unique string of numbers or letters that they have been provided with. Once the OTP has been used, it becomes invalid and cannot be used again, thus ensuring that the authentication process is secure and cannot be compromised.

OTP is considered a more secure method of authentication as compared to traditional passwords that can be easily hacked or guessed. It is commonly used in online banking, e-commerce, and other systems that require high-security measures to protect users' sensitive information.

2) Authentication using ECC

ECC (Elliptic Curve Cryptography) is a form of public-key cryptography that is commonly used in applications that require high security, such as the Internet of Things (IoT) and wireless sensor networks (WSNs).

One of the key advantages of ECC is that it provides strong security while using smaller key sizes compared to traditional public-key cryptography methods like RSA. ECC is a powerful tool for providing strong security in a wide range of applications, and when implemented correctly, it can offer an effective and efficient way to protect sensitive data and communications.

3) Authentication based on ID and Password

Setting strong passwords for accessing your IoT devices is crucial to ensure the security and privacy of your data and devices. Hackers and cybercriminals are always looking for vulnerabilities in IoT devices and weak passwords are often one of the easiest ways for them to gain unauthorized access.

4) Authentication based on certificates

Certificates are important security measures that can be used to protect IoT devices and networks. Certificates are digital documents that are used to verify the identity of devices and individuals on a network. They are typically issued by a trusted third party, such as a certificate authority (CA), and contain information about the device or individual, as well as a unique digital signature that can be used to verify the certificate's authenticity. By using certificates, devices on a network can be authorized to communicate with each other, and any unauthorized devices can be prevented from accessing the network. Certificates and PKI are powerful tools for securing IoT devices and networks, and can help to prevent unauthorized access and data breaches.

II . RELATED WORK

The open environment of the IoT, which involves a large number of heterogeneous devices communicating with each other, is vulnerable to various security threats. One important security measure to protect against these threats is authentication.

Authentication is the process of verifying the identity of a user or device attempting to access a system or network. In the context of the IoT, authentication schemes must be applied to ensure that only authorized devices and users can communicate with each other. Without proper authentication, malicious actors could impersonate legitimate

devices or users, gain unauthorized access to sensitive data or systems, and carry out various attacks such as data theft, espionage, or sabotage.

There are various authentication schemes that can be used in the IoT, including password-based authentication, public key infrastructure (PKI), and digital certificates. These schemes rely on cryptographic techniques to ensure the confidentiality and integrity of data, and to prevent unauthorized access.

In addition to authentication, other security measures such as encryption, access control, and device management are also important for ensuring the security and privacy of IoT systems. By implementing a comprehensive security strategy that includes multiple layers of protection, IoT stakeholders can minimize the risk of security breaches and ensure the trust and reliability of their systems.

The author has provided minimum user intervention to give mutual authentication between the devices, outside secret key is not needed to inject. The secret key is not stored by using any extra space; therefore, it improves the security by blocking the source of different threats [1].

Author has used hash function to provide recent authentication scheme for cloud computing, as well as these are suitable for IoT devices. These IoT devices has limited storage abilities and computation. The proposed scheme is resistance to some attacks like a forgery, user tracking, insider, desynchronization attacks [2].

Author has presented mutual authentication scheme using multi password or multi key. They used secure vault which means the secret shared between IoT smart devices and server. This secure vault has equal sized keys collection. The contents are initially shared between the server and IoT smart device, for every new session the secure vault gets changed. To prove the proposed algorithm is compatible or feasible on IoT devices they implemented on Arduino devices [3].

RFID tags are used to provide mutual authentication between IoT devices and server using elliptic curve cryptography. Performance and security analysis is done to ensure confidentiality, mutual authentication, forward secrecy confidentiality. They have not worked to overcome Spam and DDoS attacks [4].

Author has mentioned authentication for devices that are continuously are in physical contact and authentication for devices that never permanently maintain physical contact. They developed WIFI which is based on human authentication system, it is used to identify users with the help of their gait. The gait patterns are captured using COTS WiFi[5].

Author has designed an authentication mechanism for device-to-device communication which is lightweight and continuously authenticates. The proposed continuous authentication is resilient to replay, cloning, man in the middle, sybil, impersonation attacks, mutual authentication [6].

This paper represents study of various authentication schemes. Multifactor authentication is used for secret splitting. The proposed system uses Diffie-Hellman algorithm, exclusive-or.

The proposed scheme uses 3 phases:

i) Initialization
ii) Registration
iii) Authentication

The scheme is resistant to authentication factor, network attacks [7].

Authors has a systematic literature review for authentication of IoT applications and networks.

They have considered open issues for researcher and developers like

i) Identity privacy and location of IoT applications.
ii) Protocols should be lightweight by considering power consumption and security.
iii) Application, Network and Perception layer should have authentication services.
iv) Scalability of IoT nodes should be considered.
v) Low power and computation cost should be considered while designing authentication protocols [8].

Authors has considered three schemes for the survey, they observed that every scheme proposed authentication mechanism using different primitives and using single server. The three schemes were lacking in providing security against DDoS and DoS [9].
Authors has selected Caskey and LEA-128-CTR algorithms for SIMD based IoT smart device authentication. They proposed a mechanism for high speed and lightweight protocol [10].
This paper has designed multiple security scheme for authentication like by considering password, certificates, one-time passwords. They used MQTT as lightweight protocol to send the data of IoT device to the cloud system [11].

Authors has presented a key hiding technique for security threats and also proposed authentication for IoT devices. This key hiding technique is for both hardware and software.

This technique is used for data encryption and decryption, authentication, without storing the required key in memory. They have mentioned different technologies of Physically Unclonable Function (PUF) based on hardware and White Box Cryptography based on software [12] .

In this article, a privacy preserving and lightweight two-factor authentication mechanism is used for IoT devices. They considered one authentication factor known as Physically Unclonable Function (PUF) [13].

In this paper, for the secure transmission of data between local server and IoT devices 2 steps hybrid security mechanism is designed.

i) Cryptosystem of IoT
ii) Cyber security of IoT

The shared key is encrypted and stored in IoT devices; this reduces the extra computational time needed for securing the key.

Security of IoT devices maintained by using self-identification and MAC address code. The changing of shared key for every execution is a critical task, this is considered as future work [14].

This paper considers access control and attribute-based authentication for IoT devices present in home. Authors has considered five entities

i) Smart sensor
ii) Emulated Smart Fridge
iii) Emulated Smart TV
iv) Smart Phone
v) Home Server

All the entities use same cryptographic implementation [15].

In this paper, has used elliptical curve cryptography and Chebyshev chaotic maps for authentication. Proposed scheme achieves integrity, confidentiality, authentication. They used open stack swift for storage of data. Authentication between Cloud, Scanner and Tag is done.

In the authentication process Chebyshev chaotic maps are used for identity authentication [16].

Authors has proposed Physical Layer (PHY) device-to-device authentication. The PHY-ID integrates with asymmetric authentication schemes. The PHY-aided method is better as compared to PUF-based authentication, since it avoids any need of implementation overhead on IoT device. The proposed method is resistance to upper layers attacks [17].

In this paper, the authors have considered IoT device features like location, battery, token and proposed a secure and fast continuous authentication mechanism for device-to-device communication. They compared static and continuous authentication mechanisms.

Informal security analysis carried out by authors are mutual authentication, forward secrecy, anonymity, backward secrecy, availability, man in the middle attack, impersonation attack, secure localization, User Tracking attack, DoS Attack [18].

Authors has designed a e-Health system for preserving privacy schemes, as well as security needed for communication. Cryptographic primitives are used for content privacy. This content privacy depends on multicast strategy, onion routing concept, fake message injection. Trusted entity selects AES algorithm. The proposed scheme encrypts data using session keys. These keys are encrypted depending on identity-based encryption [19].

Table 2: Study of previous authentication schemes

Reference No.	Authentication Type	Cryptography Algorithm	Authentication is "IoT Device to IoT Device" or "IoT Device to Cloud"	Advantages	Limitations
[4]	Static	Elliptical Curve Cryptography	RFID tags and Server	Scalable, better security with lower resources, mutual authentication, confidentiality, non-tracking, and forward secrecy	Vulnerable to DDoS and Spam attacks
[5]	Continuous		Keyboards, mice, touchscreens		An attacker can potentially read Wi-Fi signals to identify victims without being detected
[6]	Continuous	Continuous-Authentication Protocol	IoT Device to IoT Device	Informal security analysis of proposed scheme using Replay attack, man in the middle attack, impersonation attack	Formally not proved the security of proposed protocol.
[7]	Static	Diffie-Hellman key exchange	IoT Device (Smart Card) to Cloud	Multifactor Biometric Authentication is used	
[9]	One-way accumulator, One Time Password	Diffie-Hellman key exchange, ECC	IoT Device to Cloud	countermeasures to resist DoS and DDoS attacks	Vulnerable to attacks other than DoS and DDoS attacks
[11]	Authentication based on Password, One Time Password, Certificates	Lightweight MQTT protocol	IoT Device to Cloud		Notifications are not given on smartphones when the attack occurs
[12]	Static	PUF (Physically Unclonable Function) technology and software-based WBC (Whitebox Cryptography) technology	IoT Device to Server	Provides a more reliable IoT device authentication scheme by using key hiding technology for authentication key management.	Vulnerable to key hiding issues

[13]	lightweight and privacy-preserving two-factor authentication scheme for IoT devices	physically unclonable functions, Fuzzy Extractor	IoT Devices	Two factor authentication protocol for IoT devices, which allows an IoT device to anonymously communicate with the server located at the data and control unit.	Vulnerable to password guessing attack
[14]	Static	AES	IoT Devices	Each IoT device can be differentiated and identified individually	Shared key might be stolen from seller or retailer
[23]	Continuous		plantar bio-data retrieval device	The pressure of plantar is unique and is remembered.	Noise, larger dataset is affecting the results
[24]	Continuous	Hash and MAC	Registration Authority is used to carry secure communication between IoT device and user.	Scalable, forward/backward secrecy, efficient	Registration Authority (Third Party) is needed.
[25]	Continuous		IoT-based Biometric Continuous Authentication	Various attacker models are considered	Computation cost is high, large dataset is needed.
[26]	Continuous	Contextual Information is used to access Home Devices	IoT based Home Devices	User involvement is needed, various security levels are considered	High dataset is needed, can be hack by insider attacker
[27]	Static	Untraceable and unclonable sensor movement using stable-PUF	IoT based Home Devices	Highly scalable, protect from replay and impersonation attack	Session hijacking, man-in-the-middle attack.
[29]	Static		IoT and Cloud		Vulnerable to replay attack, high communication and computation cost

The main contribution of this research is:

- We design a Cloud to IoT authentication which helps in utilizing the features of IoT devices like battery capacity, token used, so we can continuously verify the devices during the active session.
- We design lightweight key session key mechanism for secure communication between cloud servers and smart IoT devices by using hash function, concatenation operation, random numbers.

III. PROPOSED MECHANISM

The proposed experimentation has set up of a home automation system using the ESP8266 and AWS cloud services is shown in Figure 2.

To control the electric bulbs and chargers, we have connected them to the sockets on the ESP8266 board. When a user clicks/toggles the ON and OFF buttons on the web browser, the ESP8266 sends a command to the AWS instance running on the AWS cloud to turn the corresponding socket ON or OFF.

The AWS instance is responsible for receiving these commands from the ESP8266 and sending them to the appropriate socket. It may also be responsible for storing data about the state of each socket (ON or OFF) and providing a web interface for users to control the sockets.

Overall, this setup allows to remotely control your home appliances using a web browser and AWS cloud services. It provides a convenient and flexible way to manage your home automation system from anywhere with an internet connection.

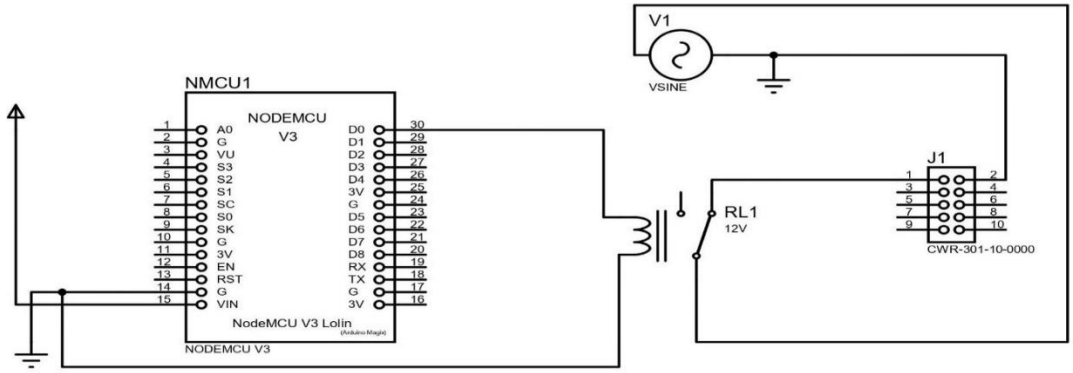

Figure 2: Node MCU ESP8266 connections for sockets

Table 3: Notations

Symbols	Description
EK_A	Encryption Key for Smart Device-A
CI_A	Cloud Identifier for Smart Device-A
DI_A	Device Identifier for Smart Device-A
E	Encrypt Message m for Smart Device-A
D	Decrypt Message m for Smart Device-A
h( )	Hash Function
$\|\|$	Concatenation Operation
DST_A	Device Session token for Smart Device-A
AT_A	Authentication Token for Smart Device-A
SK	Session Key
CST	Cloud Session Token for Cloud Server

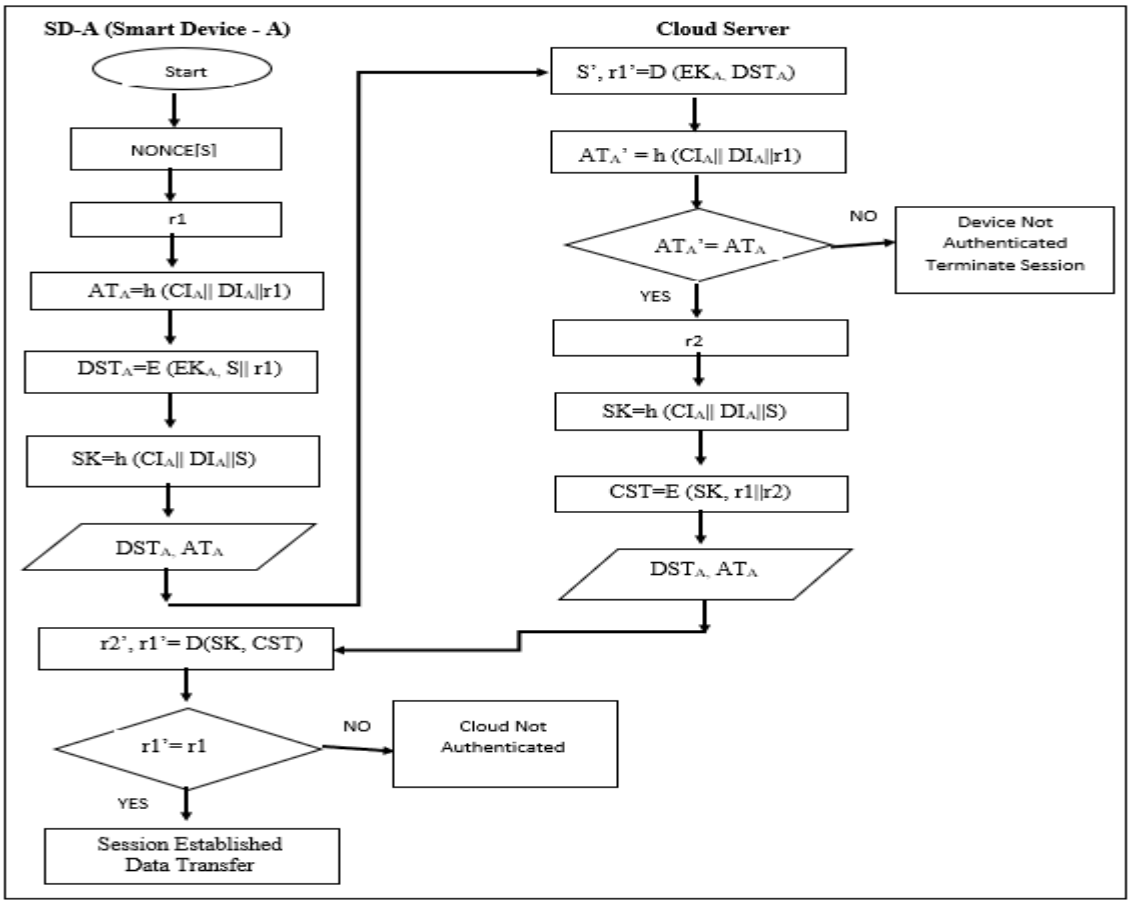

Figure 3: Flowchart of our proposed mechanism

- Generating a NONCE[S] (a unique value used for authentication) at the smart IoT device (SD-A) and including a random number (r1) in the calculation of the message authentication token can help to improve the security of the system. By including a NONCE[S] in the authentication process, it becomes more difficult for an attacker to intercept and replay the communication between the devices, as the NONCE[S] value will change with each session.
- Including a random number (r1) in the calculation of the message authentication token provides an added layer of security.
- Using a hash function (h) to calculate the authentication token can help to ensure the integrity of the message being sent by the device.

AT_A=h (CIA || DI_A || r1) where AT_A=Authentication Token of Smart IoT Device A

- Including the cloud identifier (CI_A) of the cloud server to which the IoT device is connected, the smart device identifier (DI_A) of the smart IoT device, and the "r1" random number in the data being hashed can help ensure that the authentication token is unique for each message and cannot be easily guessed or predicted by an attacker.
- Computing a Device Session Token (DST_A) using an encryption key (EK_A) for the smart IoT device (SD-A) with a NONCE=S and a random number=r1 can help establish a secure session between the device and the cloud server.
- Encrypting data (S) and the random number (r1) using the encryption key (EKA) can ensure that the information is kept confidential and only authorized entities with the key can decrypt it.

DST_A = E(EKA, S||r1) where DST_A is Calculation of Device Session token

- The cloud server receives both the Device Session Token (DST_A) and Authentication Token (AT_A) generated by a Smart IoT device (SD-A).
- The cloud server would need to have access to the encryption key in order to decrypt the DST_A (presumably encrypted data) and extract the nonce (S') and random number (r1').

S', r1'=D (EK_A, DST_A)

- The cloud server receives a message from the smart IoT device containing the Device Identifier (DI_A) and an Authentication Token (AT_A).
- The cloud server retrieves its own Cloud Identifier (CI_A) and generates a random number (r1).

- Using the retrieved values, the cloud server calculates its own version of the Authentication Token (AT_A') using a predefined formula or algorithm. This formula likely includes the CI_A, DI_A, and r1.
- The cloud server compares its calculated AT_A' value with the received AT_A value from the smart IoT device.
- If $AT_A' = AT_A$, the cloud server determines that the smart IoT device is authenticated and trusted.
- If $AT_A' != AT_A$, the cloud server determines that the smart IoT device is not authenticated and is not trusted.
- Overall, this authentication process helps to prevent unauthorized smart IoT devices from accessing the cloud server's resources and ensures that only authenticated devices are allowed to communicate with the server.

$$\mathbf{AT_A' = h\ (CI_A \,||\, DI_A \,||\, r1)}$$

the cloud server is generating a Session Key (SK) to establish a secure communication channel with the smart IoT device. Here's how the process generally works:

- The cloud server generates a new random number (r2).
- Using the Cloud Identifier (CI_A), Device Identifier (DI_A), and the previously extracted nonce (S') from the received message, the cloud server calculates the Session Key (SK) using a hash function.
- The newly generated Session Key (SK) is then sent to the smart IoT device using a secure channel.

$$\mathbf{SK = h\ (CI_A \,||\, DI_A \,||\, S')}$$

- The cloud server is generating a Cloud Server Token (CST) and encrypting it to further secure the communication channel with the smart IoT device. Here's how the process generally works: Using the newly generated Session Key (SK), the random number (r1) received in the earlier message from the smart IoT device, and the new random number (r2) generated by the cloud server, the cloud server calculates the Cloud Server Token (CST) using a predefined formula or algorithm. This formula likely involves combining and manipulating the input values in a specific way to generate a unique CST.

$$\mathbf{CST = E\ (SK, r1||r2)}$$

In Figure 4. the authentication token for smart IoT device -A (i.e., $AT_{A)\ is}$ hashed with cloud identifier and device identifier (i.e., CI_A and $DI_{A)}$ with random number r1. The cloud server receives this authentication token and calculates its own authentication token (i.e., AT_A'). These both authentication tokens are compared if they are equal then the Smart IoT device is authenticated.

We check the random number r1'and r1, if they are equal then the cloud server is authenticated and the transfer of data takes place.

IV. RESULTS AND DISCUSSION:

In terms of computation cost, our proposed protocol outperforms all the competitors. This is because we use efficient cryptographic primitives that require minimal computation. Specifically, we utilize symmetric-key cryptography to reduce the computational burden on resource-constrained IoT devices.

In terms of communication cost, our proposed protocol also performs well. We use a lightweight message exchange mechanism that minimizes the number of messages exchanged between IoT devices during the authentication process. This reduces the communication overhead, which is critical for IoT devices that have limited communication bandwidth and battery life.

Regarding authentication requirements, our proposed protocol satisfies all the key requirements of the IoT environment, including mutual authentication, freshness, integrity, and confidentiality. We also incorporate revocation mechanisms to handle compromised devices and prevent replay attacks.

Regarding security properties, our proposed protocol is robust against various attacks, including eavesdropping, man-in-the-middle attacks, and replay attacks. We use random nonces and session keys to prevent replay attacks, and we use secure cryptographic mechanisms to prevent eavesdropping and man-in-the-middle attacks.

Figure 4. represents the mutual authentication of Smart IoT Device and Cloud Server before any data transfer takes place.

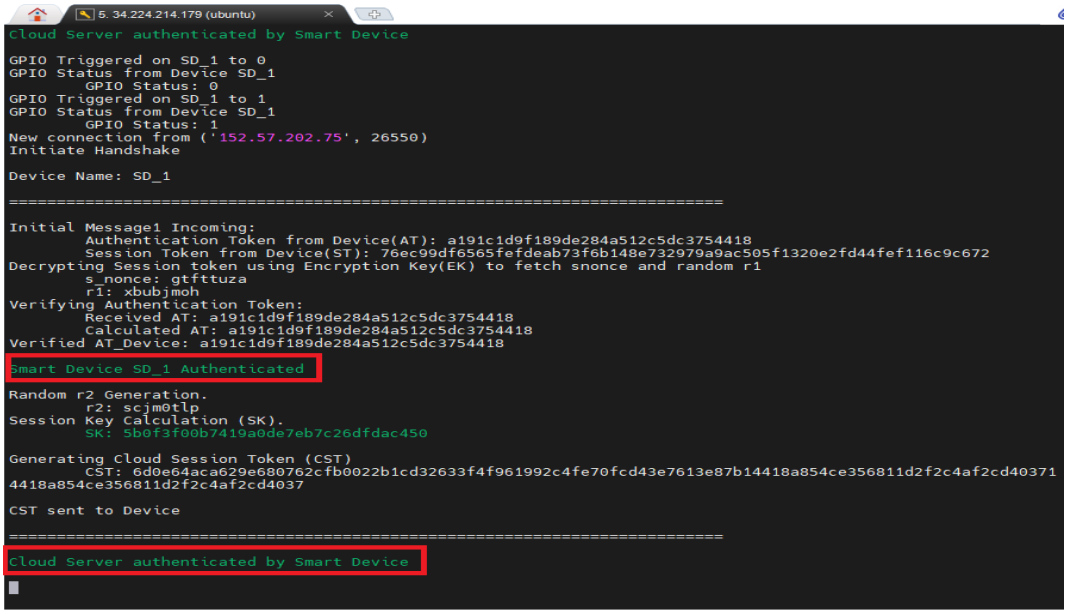

Figure 4. Mutual Authentication of Smart IoT Device and Cloud Server

Figure 5 and 6. represents that Session Key and random numbers are freshly continuously generated until the communication between IoT Device and Cloud Server continues. First the mutual authentication takes place and the session key is generated freshly after every 2 minutes till the connection terminates.

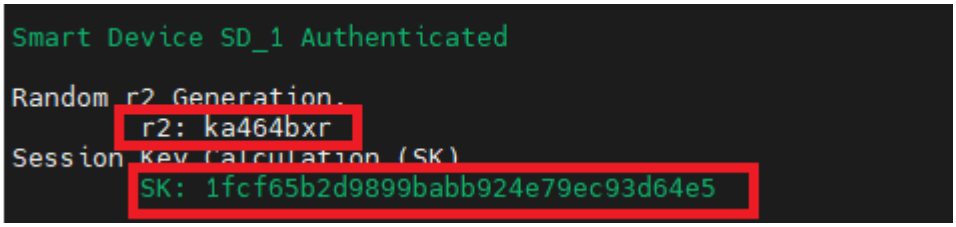

Figure 5. Screenshot of random number and session key generated at mutual authentication

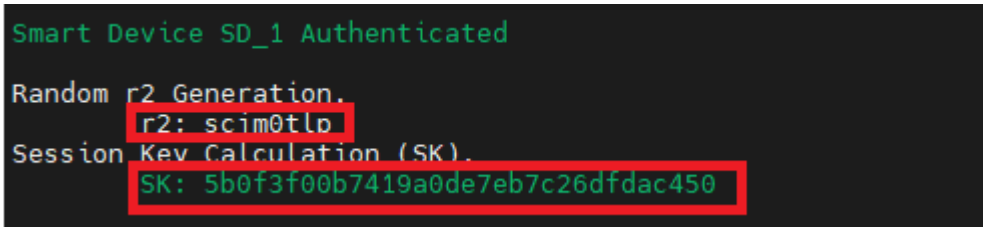

Figure 6. Screenshot of random number and session key generated continuously and freshly until the connection is active

A. Requirements for Authentication

The table 4. represents comparison of various authentication mechanisms required for IoT with our proposed mechanism.

Table 4: Comparison of authentication requirements

Requirements	[31]	[36]	[40]	[41]	[42]	Proposed
Continuous Authentication	×	√	×	×	√	√
D2D	√	√	√	√	√	√
IoT 2 Cloud	×	×	×	×	×	√
Mutual Authentication	√	√	√	√	√	√
Performance	HIGH	MEDIUM	LOW	LOW	MEDIUM	MEDIUM

B. Computation Cost

The Table 5. represents the comparison of the computation cost of proposed mechanism with another mechanisms, for our proposed mechanism we require one encryption and one decryption, one message authentication code, and two hashing functions are needed for cryptographic operations.

In comparison to our competitors, [31] and [41] have relatively high computation costs and communication overhead, which makes them less suitable for resource-constrained IoT devices. [39] has lower computation and communication costs than [31] and [41], but it only supports continuous authentication and does not provide revocation mechanisms. [40] has low computation and communication costs, but it only supports one-way authentication, which is not suitable for applications that require mutual authentication.

Table 5: Comparison of Computation cost with another mechanism/scheme

Schemes	**[43]**	**[44]**	**[45]**	**[46]**	**Proposed**
Cryptosystem	1E+1D	-	4E+4D	1E+1D	1E+1D
MAC	1 MAC	-	7 MAC	-	1 MAC
Hash Operation	1H	4H	5H	4H	2H

C. Communication Cost

The computation of communication cost by counting the number of bits transferred during the authentication process is a common approach. However, the exact method of calculating the communication cost can vary depending on the specific authentication protocol being used.

The communication cost of an authentication process can be computed by summing the number of bits transmitted between the parties during the exchange. This includes any messages sent by the initiator, any responses sent by the responder, and any additional messages required by the protocol.

We assume the lengths of random numbers(r1,r2,r1',r2',S) , Secret Keys(EK,SK),Tokens(CST,DST,AT,AT') and ID's (CI ,DI) are all of 128 bits.

The total number of bits transferred bits are computed by considering the sum of all tokens, ID's, random numbers, keys transferred during the session. The total communication cost for our protocol is 1536 in terms of bits transferred.

Table 6: Comparison of Communication cost with another mechanism/scheme

Mechanisms/Schemes	**Continuous Authentication Total bits**	**Messages**
[40]	1024	3
[41]	2464	5
[31]	4352	4
[36]	3968	4
[42]	4864	4
Proposed Mechanism	1536	3

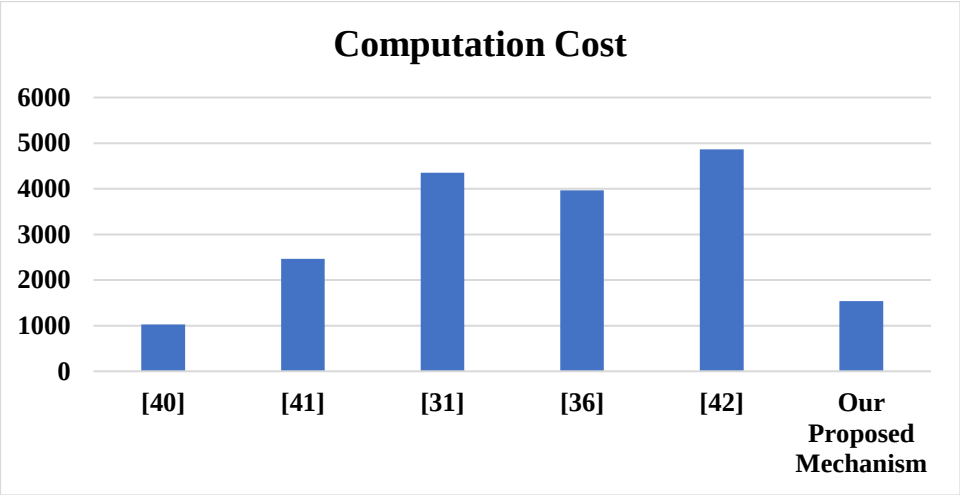

Figure 7: Comparison of computation cost with another mechanism and proposed mechanism

V. CONCLUSION

The proposed research highlights the importance of securing IoT devices by designing a cloud-to-device continuous authentication protocol. The protocol takes into consideration the hardware and software limitations of IoT devices by using lightweight cryptography functions such as hash and utilizes the device's features such as token, battery for continuous authentication. An important aspect of the protocol is its ability to preserve the privacy of the communicated devices by using anonymity and untrace ability. This ensures that the devices are not vulnerable to attacks that compromise their identity.

We generated a session key after every 2minutes until the connection is active, also random numbers are generating freshly for every new session.

Future work:

The suggested improvements can indeed enhance the security of the IoT devices and systems.

1) To notify on mobile whenever a threat, vulnerability gets occurred.

2) Location of the IoT devices should be considered in case of wearable devices.

REFERENCES

[1] S. Yoon, B. Kim, Y. Kang and D. Choi, "PUF-based Authentication Scheme for IoT Devices," *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 2020, pp. 1792-1794, doi: 10.1109/ICTC49870.2020.9289260.

[2] F. Wu, X. Li, L. Xu, A. K. Sangaiah and J. J. P. C. Rodrigues, "Authentication Protocol for Distributed Cloud Computing: An Explanation of the Security Situations for Internet-of-Things-Enabled Devices," in *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 38-44, Nov. 2018, doi: 10.1109/MCE.2018.2851744.

[3] T. Shah and S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 819-824, doi: 10.1109/TrustCom/BigDataSE.2018.00117.

[4] A. Tewari and B. B. Gupta, "A Mutual Authentication Protocol for IoT Devices Using Elliptic Curve Cryptography," *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2018, pp. 716-720, doi: 10.1109/CONFLUENCE.2018.8442962.

[5] M. Shahzad and M. P. Singh, "Continuous Authentication and Authorization for the Internet of Things," in *IEEE Internet Computing*, vol. 21, no. 2, pp. 86-90, Mar.-Apr. 2017, doi: 10.1109/MIC.2017.33.

[6] S. W. A. Shah, N. F. Syed, A. Shaghaghi, A. Anwar, Z. Baig and R. Doss, "Towards a Lightweight Continuous Authentication Protocol for Device-to-Device Communication," *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, pp. 1119-1126, doi: 10.1109/TrustCom50675.2020.00148.

[7] R. H. Shah and D. P. Salapurkar, "A multifactor authentication system using secret splitting in the perspective of Cloud of Things," *2017 International Conference on Emerging Trends & Innovation in ICT (ICEI)*, 2017, pp. 1-4, doi: 10.1109/ETIICT.2017.7977000.

[8] El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* **2019**, *19*, 1141. https://doi.org/10.3390/s19051141

[9] K. S. Roy and H. K. Kalita, "A Survey on Authentication Schemes in IoT," *2017 International Conference on Information Technology (ICIT)*, 2017, pp. 202-207, doi: 10.1109/ICIT.2017.56.

[10] S. Choi, J. Ko and J. Kwak, "A Study on IoT Device Authentication Protocol for High Speed and Lightweight," *2019 International Conference on Platform Technology and Service (PlatCon)*, 2019, pp. 1-5, doi: 10.1109/PlatCon.2019.8669418.

[11] D. K. Sharma, N. Baghel and S. Agarwal, "Multiple Degree Authentication in Sensible Homes basedon IoT Device Vulnerability," *2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*, 2020, pp. 539-543, doi: 10.1109/PARC49193.2020.236671.

[12] B. Kim, S. Yoon, Y. Kang and D. Choi, "Secure IoT Device Authentication Scheme using Key Hiding Technology," *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 2020, pp. 1808-1810, doi: 10.1109/ICTC49870.2020.9289309.

[13] P. Gope and B. Sikdar, "Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices," in *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580-589, Feb. 2019, doi: 10.1109/JIOT.2018.2846299.

[14] [Jian, MS., Wu, J.MT. Hybrid Internet of Things (IoT) data transmission security corresponding to device verification. *J Ambient Intell Human Comput* (2021). https://doi.org/10.1007/s12652-021-03122-y

[15] A. L. Maia Neto, Y. L. Pereira, A. L. F. Souza, I. Cunha and L. B. Oliveira, "Demo Abstract: Attributed-Based Authentication and Access Control for IoT Home Devices," *2018 17th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2018, pp. 112-113, doi: 10.1109/IPSN.2018.00019.

[16] C. Guntuku and S. K. Pasupuleti, "Secure Authentication Scheme for Internet of Things in Cloud," *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2018, pp. 1-7, doi: 10.1109/IoT-SIU.2018.8519890.

[17] P. Hao, X. Wang and W. Shen, "A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication," in *IEEE Access*, vol. 6, pp. 42279-42293, 2018, doi: 10.1109/ACCESS.2018.2859781.

[18] A. Badhib, S. Alshehri and A. Cherif, "A Robust Device-to-Device Continuous Authentication Protocol for the Internet of Things," in *IEEE Access*, vol. 9, pp. 124768-124792, 2021, doi: 10.1109/ACCESS.2021.3110707.

[19] R. Boussada, M. E. Elhdhili and L. A. Saidane, "Privacy Preserving Solution for Internet of Things with Application to eHealth," *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, 2017, pp. 384-391, doi: 10.1109/AICCSA.2017.75.

[20] [20] S. Khan and R. K. Aggarwal, "Efficient Mutual Authentication mechanism to Secure Internet of Things (IoT)," *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, 2019, pp. 409-412, doi: 10.1109/COMITCon.2019.8862196.

[21] P Rajesh, Mansoor Alam, Mansour Tahernezhadi, T Ravi Kumar and Vikram Phaneendra Rajesh, "Secure Communication across the Internet by Encrypting the Data using Cryptography and Image Steganography" International Journal of Advanced Computer Science and Applications (IJACSA), 11(10), 2020. http://dx.doi.org/10.14569/IJACSA.2020.0111057

[22] https://www.sinch.com/blog/one-time-password/

[23] K.-H. Yeh, C. Su, W. Chiu, and L. Zhou, ''I walk, therefore i am: Continuous user authentication with plantar biometrics,'' IEEE Commun. Mag., vol. 56, no. 2, pp. 150–157, Feb. 2018.

[24] O. O. Bamasag and K. Youcef-Toumi, ''Towards continuous authentication in Internet of Things based on secret sharing scheme,'' in Proc. Workshop Embedded Syst. Secur. (WESS). New York, NY, USA: ACM, Oct. 2015, pp. 1:1–1:8, doi: 10.1145/2818362.2818363.

[25] P. Peris-Lopez, L. González-Manzano, C. Camara, and J. M. de Fuentes, ''Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things,'' Future Gener. Comput. Syst., vol. 81, pp. 67–77, Apr. 2018. [Online]. Available: http://www. sciencedirect.com/science/article/pii/S0167739X17300407

[26] Y. Ashibani, D. Kauling, and Q. H. Mahmoud, ''Design and implementation of a contextual-based continuous authentication framework for smart homes,'' Appl. Syst. Innov., vol. 2, no. 1, pp. 1–20, 2019. [Online]. Available: http://www.mdpi.com/2571-5577/2/1/4

[27] P. Gope and T. Hwang, ''Untraceable sensor movement in distributed IoT infrastructure,'' IEEE Sensors J., vol. 15, no. 9, pp. 5340–5348, Sep. 2015.

[28] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, ''A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment,'' Future Gener. Comput. Syst., vol. 78, pp. 1005–1019, Jan. 2018. [Online]. Available: http://www. sciencedirect.com/science/article/pii/S0167739X1630824X

[29] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, ''Lightweight IoTbased authentication scheme in cloud computing circumstance,'' Future Gener. Comput. Syst., vol. 91, pp. 244–251, Feb. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X18307878

[30] H. Kim and E. A. Lee, ‘‘Authentication and authorization for the Internet of Things,’’ IT Prof., vol. 19, no. 5, pp. 27–33, 2017.

[31] P. Gope, R. Amin, S. K. H. Islam, N. Kumar, and V. K. Bhalla, ‘‘Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment,’’ Future Gener. Comput. Syst., vol. 83, pp. 629–637, Jun. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17313043

[32] Mona, J. ., Abdulzhraa Al-Sagheer, R. H. ., & Alghazali, S. . (2023). Software Quality Assurance Models and Application to Defect Prediction Techniques. International Journal of Intelligent Systems and Applications in Engineering, 11(1), 169 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2455

[33] M. Safkhani and A. Vasilakos, ‘‘A new secure authentication protocol for telecare medicine information system and smart campus,’’ IEEE Access, vol. 7, pp. 23514–23526, 2019.

[34] P. Nespoli, M. Zago, A. H. Celdran, M. G. Perez, F. G. Marmol, and F. J. G. Clernente, ‘‘A dynamic continuous authentication framework in IoT-enabled environments,’’ in Proc. 5th Int. Conf. Internet Things, Syst., Manage. Secur., Oct. 2018, pp. 131–138

[35] D. Ekiz, Y. S. Can, Y. C. Dardagan, and C. Ersoy, ‘‘Can a smartband be used for continuous implicit authentication in real life,’’ IEEE Access, vol. 8, pp. 59402–59411, 2020.

[36] J. Wang, M. Ni, F. Wu, S. Liu, J. Qin, and R. Zhu, ‘‘Electromagnetic radiation based continuous authentication in edge computing enabled Internet of Things,’’ J. Syst. Archit., vol. 96, pp. 53–61, Jun. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1383762118304491

[37] Y.-H. Chuang, N.-W. Lo, C.-Y. Yang, and S.-W. Tang, ‘‘A lightweight continuous authentication protocol for the Internet of Things,’’ Sensors, vol. 18, no. 4, pp. 1–26, 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/4/1104

[38] M. Naeem, S. Chaudhry, K. Mahmood, M. Karuppiah, and S. Kumari, ‘‘A scalable and secure rfid mutual authentication protocol using ecc for Internet of Things,’’ Int. J. Commun. Syst., vol. 33, p. 13, Jan. 2019.

[39] Muhammad Ahmad Baballe, Mustapha Aliyu Yusif, Abuhuraira Ado Musa, Nafi’u Shehu Mohammed, Mukhtar Ibrahim Bello, Abdulhamid Shariff Mahmoud, Rukayya Jafar Suleiman, & Usman Bukar Usman. (2023). Advantages and Challenges of Remanufactured Products’. Acta Energetica, (01), 01–07. Retrieved from https://www.actaenergetica.org/index.php/journal/article/view/480

[40] S. Izza, M. Benssalah, and K. Drouiche, ‘‘An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment,’’ J. Inf. Secur. Appl., vol. 58, May 2021, Art. no. 102705. [Online]. Available: https://www.sciencedirect.com/science/article/pii/ S2214212620308516

[41] A. Badhib, S. Alshehri and A. Cherif, "A Robust Device-to-Device Continuous Authentication Protocol for the Internet of Things," in *IEEE Access*, vol. 9, pp. 124768-124792, 2021, doi: 10.1109/ACCESS.2021.3110707.

[42] Proposal and Evaluation of a Dynamic Path Finding Method Using Potential Values Considering Time Series in Automatic Driving. (2022). Advances in the Theory of Nonlinear Analysis and Its Application, 6(4), 460-475. https://atnaea.org/index.php/journal/article/view/169

[43] Y. Li, “Design of a key establishment protocol for smart home energy management system,” in Proc. 5th Int. Conf. Comput. Intell., Commun. Syst. Netw. (CICSyN), Jun. 2013, pp. 88–93

[44] B. Vaidya, D. Makrakis, and H. T. Mouftah, “Device authentication mechanism for smart energy home area networks,” in Proc. IEEE Int. Conf. Consum. Electron. (ICCE), Jan. 2011, pp. 787–788.

[45] K. Han, J. Kim, T. Shon, and D. Ko, “A novel secure key paring protocol for RF4CE ubiquitous smart home systems,” Pers. Ubiquitous Comput., vol. 17, no. 5, pp. 945–949, Jun. 2013

[46] Jebri, S., Ben Amor, A., Abid, M. *et al.* Enhanced Lightweight Algorithm to Secure Data Transmission in IoT Systems. *Wireless Pers Commun* **116**, 2321–2344 (2021). https://doi.org/10.1007/s11277-020-07792-3