Sci. Educ. Innov. Context Mod. Probl. P-ISSN: 2790-0169 E-ISSN: 2790-0177
Issue 1, Vol. 8, 2025, IMCRA

Article

Secure Communication of Cloud and IoT using Lightweight Key mechanism

Gaikwad Vidya Shrimant

gaikwad.vidya30@gmail.com, ORCID: 0000-0001-9785-9249
[1] Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

Gudapati Syam Prasad

syamprasad.gudapati@gmail.com, ORCID: 0000-0002-0179-096X
Supervisor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. Working as Professor and HOD, Department of IT, Narasaraopeta Engineering College, Narasaraopet, India

Received date: 11.12.2024; Accepted date: 26.02.2025; Publication date: 06.04.2025

doi: 10.56334/sei/8.1.56

Abstract:

Internet of Things is the new technology in the field of telecommunication. IoT is progressing in the wireless, remote communication. In IoT all the smart devices create a network send and receive data through the Cloud. IoT smart devices communicate with Cloud always. In this Cloud IoT environment challenges identified are device battery life, storage space, and power consumption of smart device, security of the data exchanged between Cloud and IoT smart devices. In this paper we discuss the design and implementation of secure communication of Cloud and IoT using Lightweight Key mechanism. We have used Symmetric Lightweight Algorithm for Cloud IoT Security. We have used Advanced Encryption Standard (AES) to speed key setup time. The integration of Cloud and IoT Security with the help of AES algorithm performs effectively and consistently in both software and hardware platforms for various environments. With the help of this integration, we can use Cloud IoT services to connect various smart devices and sensors so that

Citation. Gaikwad V.Sh., Gudapati S.P. (2025). Secure Communication of Cloud and IOT using Lightweight Key mechanism. *Science, Education and Innovations in the Context of Modern Problems*, 8(1), 849-866. doi: 10.56352/sei/8.1.56. https://imcra-az.org/archive/356-science-education-and-innovations-in-the-context-of-modern-problems-issue-1-volviii-2025.html

the sensor readings are shared with others by reducing the security challenges. We have securely authenticated cloud server and IoT smart device before the communication or transfer of data gets started and also, we have generated different session keys for every new session or handshaking between them. Finally, we discuss the Cloud Computing contribution in IoT technology for the secure communication by overcoming some security challenges.

Keywords: Light weight key establishment, smart device, IoT-cloud security, authentication, AWS cloud platform, Advanced Encryption Standard.

Introduction

Internet of things is booming now days for the betterment of our life. In Internet of Things many numbers of various devices are connected to communicate with each other as well as to communicate with the cloud. Now a days, since all the devices are interconnected the data flows from each and every device, here security is the most challenging part used for transformation of data from devices to devices as well as from cloud to device or vice versa. Recent years there is rise in the development and research in lightweight key establishment algorithms for implementations on IoT devices.

The factors like low-power consumption, low cost, efficient end-to-end communication, applicability of lower resource device is considered for designing lightweight cryptography or lightweight key establishment.

In this paper, we proposed a novel lightweight key establishment mechanism between smart IoT device and Cloud. The proposed scheme addresses security threats, encryption and decryption of data. In IoT, the smart devices are communicating with the cloud and also with other devices without or less involvement of human intervention. Now a days many attacks or unauthorized access to the smart devices and attacks on data exchanged between cloud and IoT are occurring due to which the network connection gets disturbed or damaged. We have used Advanced Encryption Standard since it is used in both software and hardware, also has high rate of speed and good features of security. We have authenticated cloud server and IoT smart devices with each other before communication takes place. A new Session Key is generated for every new session between cloud and IoT device. Every smart device and Cloud Server are assigned Unique identifiers so that we authenticate them before in handshaking. Random nonce and random numbers are generated by smart device for randomness of data. Authentication Token, Device Session token are sent to cloud server by IoT device. In device Session Token we used Encryption using encryption key, nonce and random number. Cloud Server decrypts the received Device Session Token. If Authentication Token of IoT device and Authentication Token computed at Cloud Server are same the IoT Device connected to Cloud Server is Authenticated.

After authentication Cloud server compute a Session Key and sends to the IoT Device. The Device Decrypts the Session Key this is used to check the authenticity of Cloud Server. Finally, we propose a novel key establishment mechanism which is lightweight between smart IoT device and cloud server using Advanced Encryption Standard (AES) algorithm. Also, we done a state-of-the-art mechanism to securely authenticate the smart IoT device to the cloud server and vice versa.

Literature Survey

(Susha Surendran, 2018) has discussed the purpose of light weight cryptography designs needed for normal block ciphers. Also, various types of attacks are studied on some of these ciphers. Comparison of performance of these ciphers on recent Windows and Embedded platform is carried out. (2018)

(Pallavi K N,2020)discussed various lightweight cryptographic algorithms for a comparative study of message security between Cloud and IoT. Also, mentioned that different algorithms have their own performance parameters based on the size of key, storage space, and number of rounds or cycles. (2020).

(Saurabh Singh,2017) has discussed lightweight cryptographic basics like hash function, lightweight block ciphers, stream ciphers, low resources device needed for IoT platform. Analysis of lightweight cryptographic algorithms id done based on features like block size, size of the key, number of cycles or rounds etc. Also, they discussed IoT architecture by considering security factors for device environment. Their main focus of research was on issues, challenges and solutions. They proposed a scheme of security with service factor to improve resource constrained of IoT environment.

(Pejman Panahi,2021), done simulations on leading devices of IoT like Raspberry Pi 3 and Arduino Mega 2560, it has become beneficial to IoT developers to decide correct IoT Platform and encryption algorithm. Authors has measured encryption and decryption performance for different data by considering execution time, energy consumption, memory usage and throughput.

(Jatinder Singh,2016), done analysis of current state of IoT Cloud is made by focusing on security considerations. Security factors for IoT in terms of cloud providers, end users and cloud tenants across different IoT technologies.

(L. Minh Dang,2019), conducted survey to study current progress in IoT and Cloud computing ,IoT applications, IoT devices and components ,and market scenario of IoT in healthcare. Also, done in-depth review on security and privacy issues of IoT, by considering types of attacks, potential threats, security-built ups for healthcare.

Issues/Gap/Open Challenges

1) Hacking of Medical Device (Type 1): If a medical device gets hacked then it can lead failure of the whole network in which other medical devices are also connected.

2) Hacking of data Communication Channel (Type 2):

Hackers can also interfere with the communication between multiple medical devices by analysing messages.

3) Hacking data of Cloud Providers and IoT device Manufacturers (Type 3)

Hackers can steal the data of device manufactures, cloud service providers, IoT service providers, a critical loss will be caused to these parties. (Dilip Kumar Sharma,2020), in this work, multiple security factors are considered for authentication of IoT device based on Password, One Time Password and Certificates. MQTT lightweight protocol is used to send device authentication information into cloud IoT system.

Issues/Gap/Open Challenges

Security vulnerabilities and security breaches are not provided as a notification. (Valmiki Siddhartha,2020), used certificates to carry out mutual authentication as well as agreement of key between multiple IoT devices for this they designed a lightweight authentication protocol. (Hittu Garg,2019), Authors has worked to securely connect any devices on cloud and users, by using Representational State Transfer (REST) API.

Minhaj Ahmad Khan1 & Khaled Salah2 [10], presented a survey of usage of cloud for students to improve skills of practical in an educational environment. Also, presented a cloud usage taxonomy for e-learning to study the contribution of usage of cloud in e-learning.

Issues/Gap/Open Challenges

If many IoT devices are deployed on a large scale then it will lead to attack of threats and vulnerabilities on the nodes. Thus, here security of IoT should be enhanced for better communication and only authenticated, authorized user should be allowed to access data of smart devices.

(Dalton Hahn,2021), discussed classification of privacy and security vulnerabilities in Intelligent Transportation System (ITS). Some challenges are discussed in privacy issues, security in ITS.

(Hyungsik Shin,2019), for any IoT device operations it is critical to minimize the energy consumption, since they use battery power and self-harvested energy sources for operations.

Therefore, authors have done review on fundamental building blocks of corrective measures to overcome the security threats in IoT.

(SungJin Yu,2019), authors worked on how to secure any IoT devices from various attacks like replay attacks, session key disclosure and user impersonation for this they proposed a lightweight three-factor authentication and secure scheme for IoT devices.

(Yo-Hsuan Chuang,2018), proposed a protocol for gateway devices and sensing devices used in IoT environment known as lightweight continuous authentication protocol. To design this protocol most important features of IoT devices and token techniques are considered to achieve the goals.

(Pankaj Kumar,2021), authors have proposed a scheme known as Secure Addressing and Mutual Addressing, which is used to protect the network from various attacks. Using this scheme, the authentication of smart medical monitoring devices is done as well as unique addressing is used for such devices. This is useful to detect or identify such devices in medical IoT network. The performance of this scheme is measured in terms of computation, communication cost, functionality and results.

(B.D. Deebak,2020), in this paper to improve the performance efficiencies by considering communication cost and computation authors has proposed a lightweight smartcard based secure authentication and key agreement (LS-BSA). It is applied on fuzzy verifier, bilinear paining and elliptic curve cryptosystems. Lightweight operations of LS-BSA are used to establish a connectivity in a network. In the environment like cloud based intelligent data computing the proposed LS-BSA may be well suited.

(Festus Hategekimana,2020), authors have proposed Isolation and Protection Mechanism (IPM) which work as separation unit between network for securing IoT devices and devices. Also, how the central cloud-based authority is used to analyse traffic using IPM is done. The IPM performance is measured in terms of runtime reconfiguration overhead, Neptune Dos attack detection and size.

Challenges:

Testing of implementation on a large increase in the number of IoT devices which are connected to the central server.

(Benfano Soewito,2021), author's has designed a security system for transmission of encrypted data.They used Advanced Encryption System for encryption purpose and Zero Knowledge Proof Algorithm for authentication. Data Transmission is divided into two processes registration process and authentication process.

i) Registration Process- here user does registration by entering username and password, but a variable Y representing as a password is sent to the server, original password is not sent to the server.

ii) Authentication Process- here user has no need to enter password again. Only the data to be encrypted is entered and send to the server. At server-side decryption on the data is done.

(Lu Zhou,2019), author presented a study of novel authentication scheme for cloud servers combined with IoT based architecture. Proposed scheme operates well when the communication data/message is short in length. This scheme has achieved security properties such as mutual authentication, user audit, session security also authentication is tested on various types of attacks and it is secure.

(Afolabi, A.O.,2016), the features like security, reliability, architecture, scalability, flexibility are considered for comparative study which are essential for secured wired and wireless communication.

Author has considered standard encryption algorithms like RSA, AES, DES, and 3DES for comparative analysis.

Performance analysis is carried out by considering

i) Power Consumption Rate
ii) Flexibility and Security
iii) Encryption Time
iv) Output Byte
v) Memory Usage.

Based on the results authors concluded that AES encryption algorithm uses least memory usage and also it consumes less encryption time.

(Jun Zhou,2017), authors have considered the next generation mobile technologies on Cloud IoT and introduced some privacy and security requirements, architecture. Also, they identified some faults in existing work. They identified the challenges in authentication, privacy and packet forwarding.

List of challenges mentioned:

i) In Cloud IoT privacy-preserving of outsourced data mining.
ii) In cloud IoT – access control of fine-grained ciphertext.

(William J. Buchanan,2017), the review of lightweight cryptography has done, also analysis of strength and weakness is done. Overview of cryptography needed for IoT, is discussed which is used for some resource limited smart devices like RFID, intelligent sensors etc.

(G. S. Prasad and V. S. Gaikwad,2018), has done survey on user awareness of cloud security.

(C. Gritti,2020), author has proposed a publicly verifiable PORR (Proofs of Retrievability and Reliability) using Verifiable Delay Functions, which are easy to verify and slow to compute.

(Gudapati, S.P., Gaikwad, V.,2021), author has proposed a lightweight key mechanism for secure communication between cloud and smart devices (IoT devices). Authentication of smart devices and cloud is done before starting every new communication. A new session is generated for every new session.

Security Properties

Properties needed for Security in IoT Cloud Environment

Recent research has identified the major security properties needed to be considered from the beginning of the connection establishment between IoT devices and Cloud environment.

1) Authentication and Authorization of User:

The IoT service platform should provide authentication to access the network of sensors, and authorization to get access a particular sensor connected to the network.

The detailed requirement is given below:

i) Uniquely identified users should register for IoT service.

ii) Every user should be authenticate using ID-based method.

iii) Error should be popped up after failure in authentication.

2) Data/Message/Information Integrity:

It ensures that the message received is the same message sent by the sender without any alteration by a hacker during transmission.

3) Lightweight protocol/mechanism:

The session key establishment and authentication should be lightweight since the security algorithms create overburden to the IoT application.

Proposed Scheme

This section, represents our proposed mechanism to establish a session key, that provide efficient security.

Table 1: Symbols used for our proposed mechanism

Symbols	Description
EK_A	Encryption Key for SD-A
CI_A	Cloud Identifier for SD-A
DI_A	Device Identifier for SD-A
$E_A[m]$	Encrypt message 'm' for SD-A
$D_A[m]$	Decrypt message 'm' for SD-A

855

h( )	Hash function
||	Concatenation Operation
DST_A	Device Session Token for SD-A
AT_A	Authentication Token for SD-A
SK	Session Key
CST	Cloud Session Token for Cloud Server
S	Nonce
r1,r2,r1',r2'	Random numbers

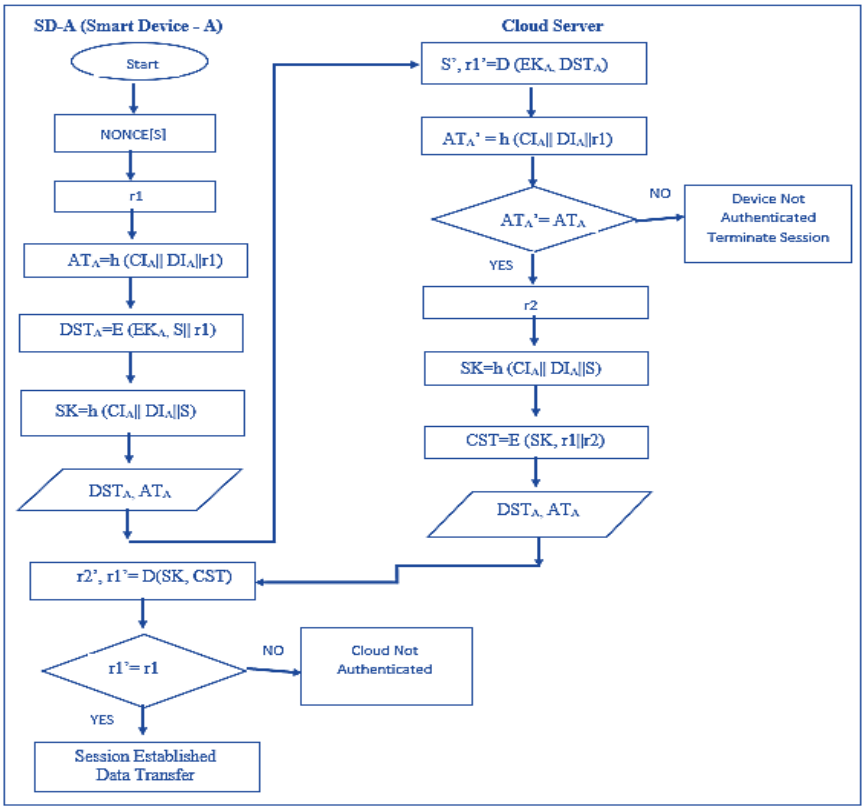

Figure 1. Flowchart of Proposed Scheme

A. Proposed scheme System Setup

Smart Device and the Cloud Server have Unique ID. The user stores the Smart device ID and Cloud ID in json file.

In this data.json file we have declared SD_1 and SD_2 are smart device 1 and 2 respectively, DI=Smart Device Identifier, GI=Cloud Server Identifier, EK=Encryption Key, Port. DI, GI and EK are 128 bits in size. Figure 2, shows the content of DI, GI, EK and PORT.

Figure 2. data.json file

Every smart device connecting to cloud should be authenticated at the start. This proposed scheme can be used in many applications/projects e.g., weather control system, transportation and logistics, monitoring machines, smart city, smart home appliances, health care.

Experimentation

Requirements

1) ESP8266
2) ESPLORER
3) AWS Management Login
4) MobaXterm

1) ESP8266

The ESP8266 is a Wi-Fi module great for IoT and Home Automation projects[24].

NodeMCU (**N**ode **M**icro **C**ontroller **U**nit) is development board and an open-source Lua based firmware used for IoT based applications, Home Automation [23].

It contains elements of a computer: CPU, RAM, networking (WiFi), and even a modern operating system and SDK [25].

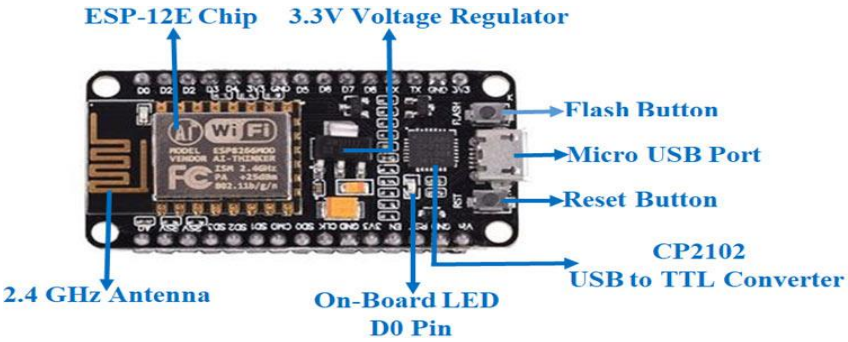

Figure 3 . ESP8266 (Mobatek. (n.d.).)

4) MobaXterm

MobaXterm is a useful **toolbox for remote computing (**Mobatek. (n.d.).).

It provides lots of functions for web developers, IT administrators, programmers in a single Windows application to handle remote jobs[26].

It provides all the important remote network tools like Secure Shell (SSH), X11 protocol designed for unix, Remote Desktop Protocol (RDP), Virtual Networking Computing (VNC), File Transfer Protocol (FTP), Mobile Shell (MOSH) and Unix commands (like awk,cat,ls,bash,grep,rsync,sed….) to Windows Desktop in a single portable exe file which works out of the box[26].

Following the steps to create a Session on MobaXterm[27]

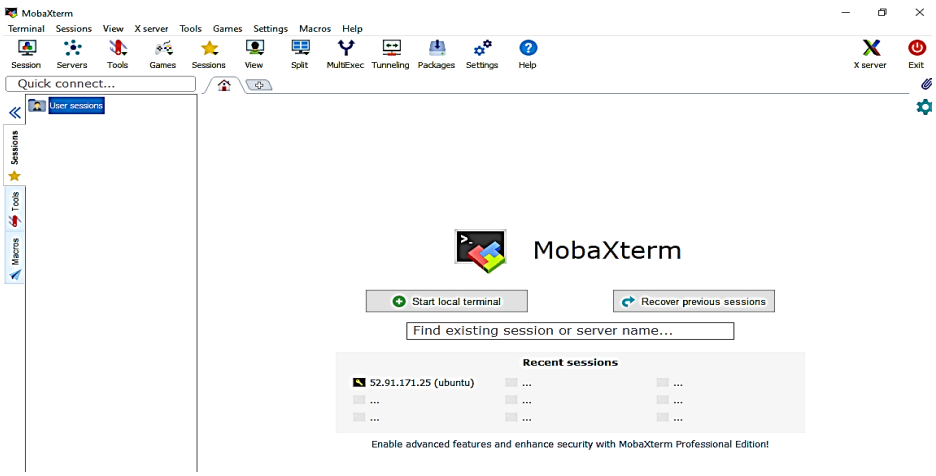

Figure 4. MobaXterm

In the MobaXterm ,click on the session, then on SSH and click on Advanced SSH settings ,select the checkbox of Use Private Key and browse the path of ubuntu.pem file .

After that login to AWS account select the instance that is running, copy the Public IPv4 address and put it in Remote Host of MobaXterm.Specify the username and enter ubuntu.

Finally click OK.

1) Type the command: cd /var/www/html/application/

2) Type python2 SmartSystemServer.py (python file containing the code)

3) Open the ESplorer.bat

4) Connect the Smart Device

5) Select COM4

6) Select 115200

7) Click on Open

8) Reset the device

9) Click on Open and select init.lua file

10)Change IP address in code with AWS public IPv4 address

11)Click on Format

12) It displays format done

13) Reset the device

14) Save the code

15) Change the name and password of Wifi device in wifi.sta.config

16) Again reset the device

17) Open MobaXterm

18) Open browser and put Public IPv4 address

19) Now click on Toggle Button to On and Off the device lights.

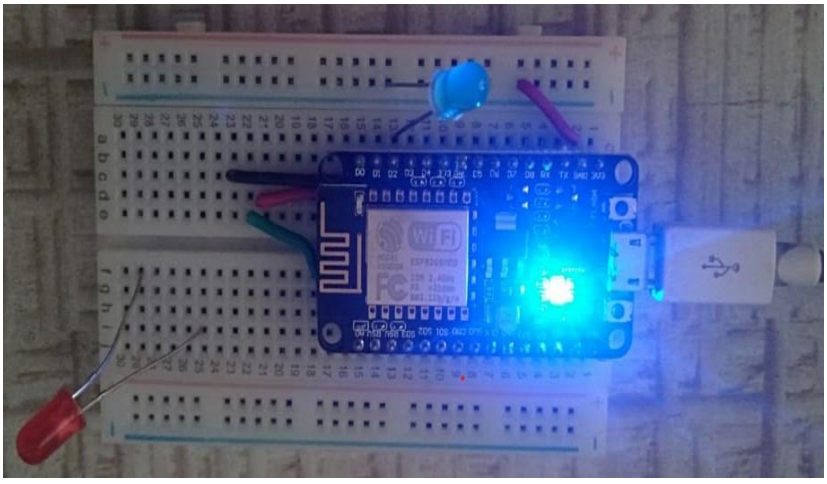

Figure 5 . ESP8266 as IoT Smart Device connected to AWS Cloud

The Figure 6. Shows the AWS Instance is in Running State and Public IPv4 is used in MobaXterm and in Lua code.

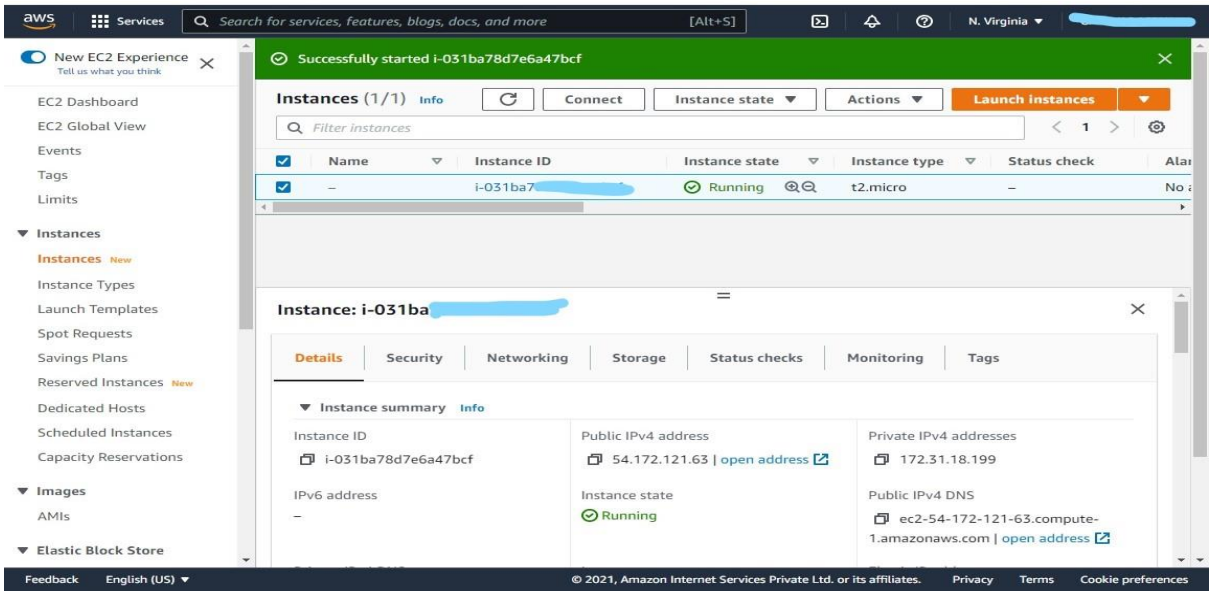

Figure 6 . AWS Running Instance

Following images shows the actual flow of proposed scheme.

1) Figure 7. shows the smart device SD_1 and SD_2 is configured on Port 9001 and Port 9000.

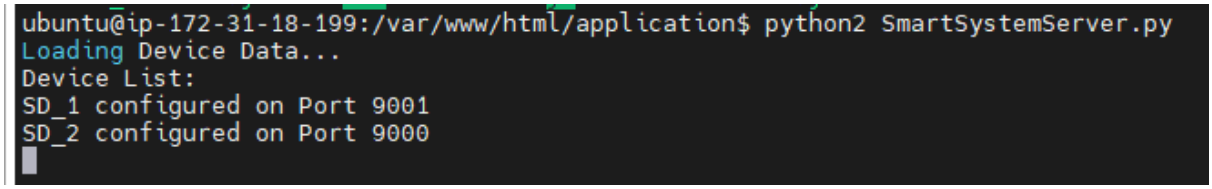

Figure 7. Commands to given in MobaXterm

2)Figure 8. represents the handshaking between smart device and cloud server, authentication of smart device, generation of session key, also cloud server authentication by smart device.

Where, SD-1 is IoT Smart Device ,r1and r2 is random number,AT is Authentication Token,CST is Cloud Session Token,SK is session Key,CST is Cloud Session Token,ST is Session Token.Authentication of Smart Device and Cloud Server is shown in the output.

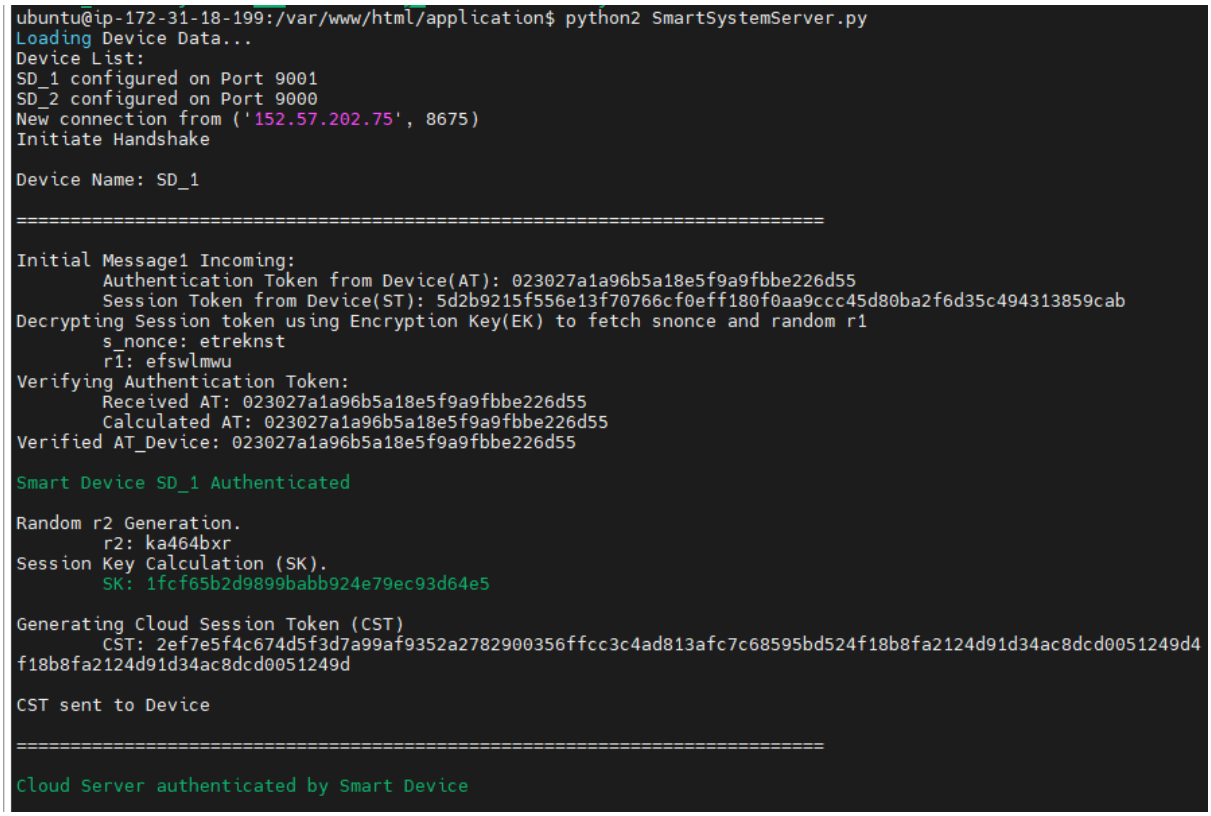

Figure 8. Proposed Scheme Output using AES algorithm

3) Figure 9. represents the browser output. Here in the browser, we have given the Public IPv4 address of AWS Instance which is running in AWS Cloud. Click on Toggle to make the led ON and OFF on ESP8266.Once the authenticity of Cloud and IoT device is checked it displays the status of SD_1(Smart Device_1) status either 1 or 0 is shown in Figure 10.

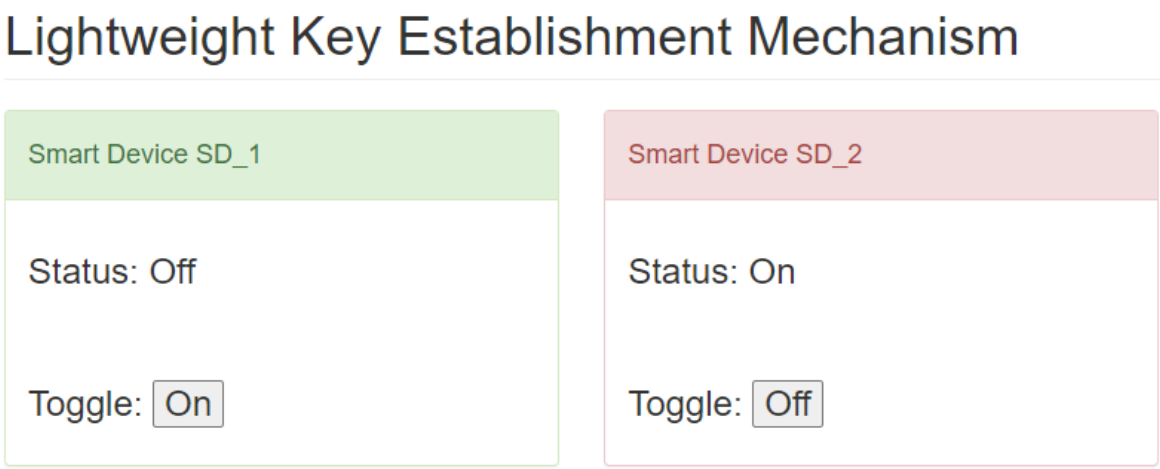

Figure 9. Browser Screenshot

```
SD_1 configured on Port 9001
SD_2 configured on Port 9000
New connection from ('152.57.202.75', 8675)
Initiate Handshake

Device Name: SD_1

================================================================================

Initial Message1 Incoming:
        Authentication Token from Device(AT): 023027a1a96b5a18e5f9a9fbbe226d55
        Session Token from Device(ST): 5d2b9215f556e13f70766cf0eff180f0aa9ccc45d80ba2f6d35c494313859cab
Decrypting Session token using Encryption Key(EK) to fetch snonce and random r1
        s_nonce: etreknst
        r1: efswlmwu
Verifying Authentication Token:
        Received AT: 023027a1a96b5a18e5f9a9fbbe226d55
        Calculated AT: 023027a1a96b5a18e5f9a9fbbe226d55
Verified AT_Device: 023027a1a96b5a18e5f9a9fbbe226d55

Smart Device SD_1 Authenticated

Random r2 Generation.
        r2: ka464bxr
Session Key Calculation (SK).
        SK: 1fcf65b2d9899babb924e79ec93d64e5

Generating Cloud Session Token (CST)
        CST: 2ef7e5f4c674d5f3d7a99af9352a2782900356ffcc3c4ad813afc7c68595bd524f18b8fa2124d91d34ac8dcd0051249d4
f18b8fa2124d91d34ac8dcd0051249d

CST sent to Device

================================================================================

Cloud Server authenticated by Smart Device

GPIO Triggered on SD_1 to 0
GPIO Status from Device SD_1
        GPIO Status: 0
GPIO Triggered on SD_1 to 1
GPIO Status from Device SD_1
        GPIO Status: 1
```

Figure 10. Status of SD_1 either 0 or 1 after pressing Toggle Button ON or OFF on browser

4) Figure 11. represents different Session Keys (SK) and random number (r2) are generated for every New Session.

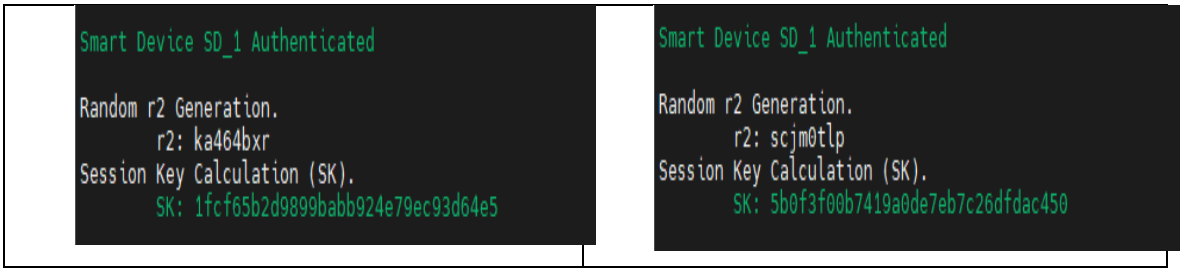

Figure 11. Different Session Key (SK) and Random Number (r2) generated for every new session

Conclusion

In this paper, we have gone through lightweight cryptographic algorithm AES for providing secure communication between Cloud Server and IoT Smart Device. This lightweight algorithm is used since they have fast speed processing, key size is smaller, less computation power is required. We achieved the authentication of Cloud Server and IoT devices communicating on network connection. Also, different session keys and random numbers are generated for every new connection establishment. In the future, we are going to provide proof-of-concept to prevention of attacks on our novel algorithm: Masquerade attack, replay attacks Message Forgery attack, Device Compromise attack, know key attack.

References

1. Afolabi, Adeolu & O.G., Atanda. (2016). Comparative Analysis of some Selected Cryptographic Algorithms. Computing information Systems, Development Informatics& Allied Research Journal. volume 7. 41-57.
2. B.D. Deebak, Fadi AL-Turjman,(2021) Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing, Future Generation Computer Systems, Volume 116, 2021, Pages 406-425, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.11.010.
3. Benfano Soewito, Yonathan Marcellinus (2021). IoT security system with modified Zero Knowledge Proof algorithm for authentication, Egyptian Informatics Journal, Volume 22, Issue 3, 2021, Pages 269-276, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2020.10.001.

B. Gritti (2020). Publicly Verifiable Proofs of Data Replication and Retrievability for Cloud Storage. 2020 International Computer Symposium (ICS), 2020, pp. 431-436, doi: 10.1109/ICS51289.2020.00091.

4. Chuang Y-H, Lo N-W, Yang C-Y, Tang S-W. (2018) A Lightweight Continuous Authentication Protocol for the Internet of Things. Sensors. 2018; 18(4):1104. https://doi.org/10.3390/s18041104.
5. DaddyShark. (2018, October 2). What is MobaXterm and how to install it on your computer for FREE. Retrieved from https://datashark.academy/what-is-mobaxterm-and-how-to-install-it-on-your-computer-for-free/
6. Dang, L. M., Piran, M. J., Han, D., Min, K., & Moon, H. (2019). A survey on Internet of things and cloud computing for healthcare. Electronics, 8(7), 768. https://doi.org/10.3390/electronics8070768
7. Dilip Kumar Sharma, Neeraj Baghel, & Siddhant Agarwal. (n.d.).(2020) Multiple Degree Authentication in Sensible Homes based on IoT Device Vulnerability. 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC).
8. G. S. Prasad and V. S. Gaikwad, (2018) "A survey on user awareness of cloud security", Int. J. of Engineering and Technology, vol. 7, no. 2.32, pp. 131-135, May 2018.
9. Getting started with ESP8266 WiFi transceiver (Review). (2020, May 17). Random Nerd Tutorials. https://randomnerdtutorials.com/getting-started-with-esp8266-wifi-transceiver-review/
10. Gudapati, S.P., Gaikwad, V. (2021). Light-Weight key establishment mechanism for secure communication between IoT devices and cloud. In Intelligent System Design (pp. 549–563). Springer, Singapore (2021)
11. Hahn, D., Munir, A., & Behzadan, V. (2021). Security and privacy issues in intelligent transportation systems: Classification and challenges. IEEE Intelligent Transportation Systems Magazine, 13(1), 181-196. https://doi.org/10.1109/mits.2019.2898973
12. Hategekimana, Festus & Whitaker, Taylor & Pantho, Md & Bobda, Christophe. (2020). IoT Device Security Through Dynamic Hardware Isolation with Cloud-Based Update. Journal of Systems Architecture. 109. 101827. 10.1016/j.sysarc.2020.101827.
13. Hittu Garg, Nit Kurukshetra, & Mayank Dave. (n.d.).(2019) Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware. 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)

14. Hyungsik Shin, Ho Kyoung Lee, Ho-Young Cha, Seo Weon Heo, & Hyungtak Kim. (2019). IoT Security Issues and Light Weight Block Cipher. 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC).
15. Jdkerr. (2019, October 3). NodeMCU ESP8266 specifications, overview and setting up. Retrieved from https://www.make-it.ca/nodemcu-arduino/nodemcu-details-specifications/
16. Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos. (2017). Security and Privacy for Cloud-Based IoT: Challenges. Comm. Mag. 55, 1 (January 2017), 26–33. DOI:https://doi.org/10.1109/MCOM.2017.1600363CM
17. K N Pallavi, V Ravi Kumar, & S Srikrishna. (2020). Comparative Study of Various Lightweight Cryptographic Algorithms for Data Security Between IoT and Cloud. 2020 5th International Conference on Communication and Electronics Systems (ICCES).
18. Khan, M. A., & Salah, K. (2019). Cloud adoption for E-lEarning: Survey and future challenges. Education and Information Technologies, 25(2), 1417-1438. https://doi.org/10.1007/s10639-019-10021-5
19. Lu Zhou, Xiong Li, Kuo-Hui Yeh, Chunhua Su, Wayne Chiu, (2019) Lightweight IoT-based authentication scheme in cloud computing circumstance, Future Generation Computer Systems, Volume 91,2019, Pages 244-251, ISSN 0167-739X,https://doi.org/10.1016/j.future.2018.08.038.
20. Mobatek. (n.d.). MobaXterm free Xserver and tabbed SSH client for Windows. https://mobaxterm.mobatek.net/
21. NodeMCU ESP8266 Pinout, specifications, features & datasheet. (n.d.). Components101 – Electronic Components Pinouts, Details & Datasheets. https://components101.com/development-boards/nodemcu-esp8266-pinout-features-and-datasheet
22. Panahi, P., Bayılmış, C., Çavuşoğlu, U., & Kaçar, S. (2021). Performance evaluation of lightweight encryption algorithms for IoT-based applications. Arabian Journal for Science and Engineering, 46(4), 4015-4037. https://doi.org/10.1007/s13369-021-05358-4
23. Pankaj Kumar, Lokesh Chouhan, (2021) A privacy and session key-based authentication scheme for medical IoT networks, Computer Communications, Volume 166,2021, Pages 154-164, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2020.11.017.

24. Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of things. IEEE Internet of Things Journal, 3(3), 269-284. https://doi.org/10.1109/jiot.2015.2460333
25. Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing. https://doi.org/10.1007/s12652-017-0494-4
26. Surendran, S., Nassef, A., & Beheshti, B. D. (2018). A survey of cryptographic algorithms for IoT devices. 2018 IEEE Long Island Systems, Applications and Technology Conferenc (LISAT). https://doi.org/10.1109/lisat.2018.8378034
27. Valmiki Siddhartha, Gurjot Singh Gaba, & Lavish Kansal. (2020, April). A Lightweight Authentication Protocol using Implicit Certificates for Securing IoT Systems [Paper presentation]. International Conference on Computational Intelligence and Data Science.
28. William J. Buchanan, Shancang Li & Rameez Asif (2017) Lightweight cryptography methods, Journal of Cyber Security Technology, 1:3-4, 187-201, DOI:10.1080/23742917.2017.1384917
29. Yu, S., Park, K., & Park, Y. (2019). A secure lightweight three-factor authentication scheme for IoT in cloud computing environment. Sensors, 19(16), 3598. https://doi.org/10.3390/s19163598