IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⧖ Impact Factor 8.102 ⧖ Peer-reviewed / Refereed journal ⧖ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125115

A Secure User Authentication Scheme For Enabled Iot Devices

Karthiga G [1], Kaviya S[2], Lavanya V[3]

DMI College of Engineering[1]

DMI College of Engineering[2]

Assistant professor, DMI college of Engineering[3]

Abstract: The internet of things is a system of connecting devices to the internet. It interacts with the real world with wide range of applications. Nowadays, in many home, user can remotely access and control a variety of home devices such as smart curtains, lights etc. despite providing convenient services including home monitoring, temperature management and daily work assistance. A smart home can be vulnerable to malicious attacks because all messages are transmitted over insecure channels. Moreover, home devices can be a target for device capture attacks since they are placed in physically accessible locations. But, IOT has a disadvantage that it has less security. To provide security for protecting information to be delivered and communication through the use of codes we use cryptography. In cryptography we are using AES algorithm, in this message will be passed in turns of block ciphers. To connect IOT and cryptography we require MQTT (message queuing telemetry transport) broker to publish and subscribe system takes place, in which we can publish and receive message as a client. This encrypted message cannot be decoded until it has decryption key, so the device can secure from attacks.

Keywords: Internet of Things (IoT), Message Queuing theory telemetry transport (MQTT), Advanced Encryption Standard (AES), Amazon web service (AWS), Light Emitting Diode(LED).

I. INTRODUCTION

In recent years, the Internet of Things (IoT) has expanded rapidly as network technology device access and related analytical systems have improved. IoT protection refers to techniques and systems designed to protect IoT infrastructure and networks. Defence against threats is still not always handled because the networking systems are viewed as accountable for the threats. IoT refers to the Internet of Things. Along with the variety of platforms and networking devices used in IoT systems, there are multiple protocols and functions that have been supplied to IoT network solutions. IoT devices aid humans by performing various functions such as detecting weather conditions, supporting hospital equipment for operations, identifying animals using biochips, and providing tracking and connectivity in automobiles. IoT servers gather data from these devices in real time and process the data to enhance the efficiency of the system. However, many view the current regulatory procedures in the United States as ineffective. The Open Web Application Security Project (OWASP) focused on the three levels of an IoT device: technology, data communications, and communication protocols. As a result, as shown in Figure, the authors concluded that the deployment of Internet security countermeasures must include security infrastructure at all IoT layers. The IoT ecosystem includes a wide range of devices, including smart home appliances, wearable devices, industrial sensors, medical devices, and more. IoT security includes various methods, techniques, and protocols used to ensure the security and privacy of IoT devices, networks, and data These devices are typically connected to the internet, making them vulnerable to various security threats such as unauthorized access, data breaches, and cyber-attacks. The security challenges of IoT are numerous and complex. IoT devices are often low-cost and low-powered, making them susceptible to security vulnerabilities such as weak authentication, lack of encryption, and susceptibility to malware.

II. LITURATURE SURVEY

[1] Internet of Things (IoT) is revolutionizing and enhancing the quality of human lives in every aspect. Today major cloud and IoT service providers including Amazon Web Services (AWS), Google Cloud Platform (GCP), and Azure utilize some customized forms of Role-Based Access Control (RBAC) model along with specific authorization policies enabled by policy-based access control models. They develop a formal attribute-based access control (ABAC) model for AWS IoT by building upon and extending previously developed access control model for AWS IoT, known as AWS-IoTAC model. We demonstrate the applicability of our proposed model through an industrial IoT use case and its implementation in the AWS IoT platform.

DOI: 10.17148/IJARCCE.2023.125115

[2] Z-Wave smart home Internet of Things devices are used to save energy, increase comfort, and remotely monitor home activities. In the past, security researchers found Z-Wave device vulnerabilities through reverse engineering, manual audits, and penetration testing. Thus, in this paper, we present Fuzz, a protocol aware Blackbox fuzzing framework for quickly assessing vulnerabilities in Z-Wave devices. Fuzz assesses the target device capabilities and encryption support to guide seed selection and tests the target for new vulnerability discovery. It uses our field prioritization algorithm (FIPA), which mutates specific Z-Wave frame fields to ensure the validity of the generated test cases.

[3] The rapid growth of the Internet of Things (IoT) has enabled prompt services over mobile devices. The Global Mobility Network (GLOMONET) is an important global network that allows mobile users to access the Internet anywhere. First, AMAPG contains large amounts of information on the smart card of the mobile phone. Therefore, they are vulnerable to attacks that steal critical information. Second, it is susceptible to password-guessing attacks. Third, AMAPG cannot guarantee the security of future messages because attackers can steal the session key. In this study, we discuss the weaknesses of AMAPG and propose a new three-factor authentication scheme called the secure mobile authentication scheme for GLOMONET (SMASG).

[4] With the increased number and reduced cost of smart devices, Internet of Things (IoT) applications such as smart home (SHome) are increasingly popular. As a result, a number of authentication solutions specifically designed for IoT environments have been proposed. First, it presents a generic model derived from an SHome use-case scenario. Secondly, based on the model, it performs a threat analysis to identify possible means of attacks. The analysis leads to the specification of a set of desirable security requirements for the design of authentication solutions for SHome. Thirdly, based on the requirements, existing authentication solutions are analysed and some ideas for achieving effective and efficient authentication in IoT environments are proposed.

[5] The information sensed by several IoT smart devices can be security stored at the (cloud) servers. Proposed a smart card based remote user authentication scheme using user password. In this comment paper, we carefully analysed the scheme of Rana et al. and tracked down that their scheme is insecure against serious attacks, including stolen smart card attack, privileged-insider attack, user impersonation attack, password change attack and Ephemeral Secret Leakage (ESL) attack. Furthermore, their scheme does not preserve untrace ability feature. To remedy these security pitfalls, we also provide some remedies that can help in building more secure and effective user authentication scheme to apply in securing next generation IoT infrastructure.

III.PROPOSED SYSTEM

To safeguard the data produced by IoT devices, numerous methods & techniques have been developed. The data produced by IoT devices is encrypted using a variety of modern security algorithms and techniques, which we have used shown below.

An instance of the Internet of Things was demonstrated by linking a few sensors. The data is received by the card designed and developed by Espressif Systems (ESP8266) module, where it is encrypted before being sent to the internet site through an authorized person to be received from anywhere. It is also feasible to acquire it via a public IP address that is disclosed within the ESP32 device module's internal network. To discover the sensors' actual values, the decryption component is finally proposed.

The Internet of Things (IoT) component was represented by a variety of sensors, including the DH11 temperature and humidity sensor, ultrasonic sensor, and LED IoT Security. Here we used LED light were connected to ESP32 using AES encryption technology. The ESP32 chip receives the data, encrypts it, and then sends it to a special internet page that must be accessed securely using a username and password. The data is also broadcast on the IP address of the ESP32 chip within the very same service provider's local Internet network. Following receipt of the data, it could be decrypted using an AES program available on the Internet & as a mobile device application to identify the real values of the data received. As a result, if someone gains access to the informational page and attempts to steal the data, determining the real values will be difficult since they will need to be knowledgeable of the encryption technique and key used in this approach. As a result, security can be strongly achieved.

The AES encryption technique was developed on the ESP32 platform and the design was also applied to numerous sensors to symbolize the IoT component of a smart home or another application. This method was created to improve and reinforce the security of the Internet of Things. We settled on a sensor with two lights. Because of the ESP32 chip's ability to communicate with IoT and the efficacy of AES technology in encrypting and safeguarding data received or delivered, this architecture might be utilised to preserve and secure incoming information from the Internet of Things.

DOI: 10.17148/IJARCCE.2023.125115

For the NodeMCU open source firmware, open source prototype board designs are available. It is a Wi-Fi capable gadget that utilizes the esp-83 Wi-Fi SoC. It features built-in Wi-Fi, which lowers the cost and facilitates remote access; once input is provided, it can also function without internet access. It sensos the code and the LED is turn on. It uses a Arduino IDE. The board contains 3 cables, current limiting resistor . In our implementation we have connected the LED to current limiting resistor, FTDI to nodeMCU respectively.

ARDUINO CODE

The data from the sensor is received by Arduino code from the sensor. It gives values. We have used the AES algorithm for encryption. The data is sent from Arduino to the mysql database after encryption then stored in 6 different columns in the database.

AES ENCRYPTION

The National Institute of Standards & Technology (NIST) of the U. S. developed the Advanced Encryption Standard (AES) in 2001 as a standard for electronic data encryption. AES is extensively used nowadays owing to its significantly better strength than DES & triple DES, although it is more difficult to construct. Instead of using a Feistel cipher, AES uses iteration. It is based on substitution & permutation networks, which are two popular approaches for encrypting & decrypting data (SPN). Block cipher algorithms perform a number of mathematical operations called SPN. AES has a constant plaintext block size of 128 bits (16 bytes). AES employs a byte matrix, which is represented as just a 4x4 matrix. Additionally, the number of rounds in AES is a critical component. The length of the key determines how many rounds there will be. The AES technique uses 3 different key sizes to decrypt & encrypt data, including (128, 192 as well as 256 bits).

Security of AES

Security was one of the most important factors taken while choosing an algorithm by NIST. The primary causes of this were evident given that one of the key goals of AES was to enhance the security flaw of the DES algorithm. When compared to other suggested algorithms, AES has the best ability to keep hackers away from sensitive data and prevents them from decrypting it. This was accomplished by extensively testing AES against both theoretical and real-world attacks.

- AES is indeed a block cipher.
- The key size might be 128/192/256 bits.
- Data is encrypted in 128-bit chunks.

Working of AES

There are three block ciphers in AES: 1. AES-128 encrypts & decrypts a block of messages with a 128-bit key length. 2. AES-192 encrypts & decrypts a block of messages using a 192-bit key length. 3. AES-256 encrypts & decrypts a block of messages using a 256-bit key length. Each code uses 128, 192, or 256-bit cryptographic keys to scramble & decode information in blocks of 128 pieces. Secret key figures, also known as symmetric figures, use the same key for both encoding and decoding. There must be a similar mystery key that both the source and the recipient are aware of and can use. The government categorizes data as secret, confidential, or top secret. Any key length can be used to secure the Confidential & Secret levels. For extremely confidential data, cycle key lengths of 192 or 256 are necessary.

Encryption

The AES encoding calculation defines numerous modifications to be done on data stored in just a cluster. The 1st stage in the code is to insert the data into an exhibit, following that the code modifications are rehashed across many encryption cycles. The first modification to the AES encoding figure is the use of an alternate table to replace information. The consequent modification moves information lines. The 3rd combines portions. A distinct component of the encryption key is used to accomplish the continuation change on each segment. Longer keys need more adjustments to finish.

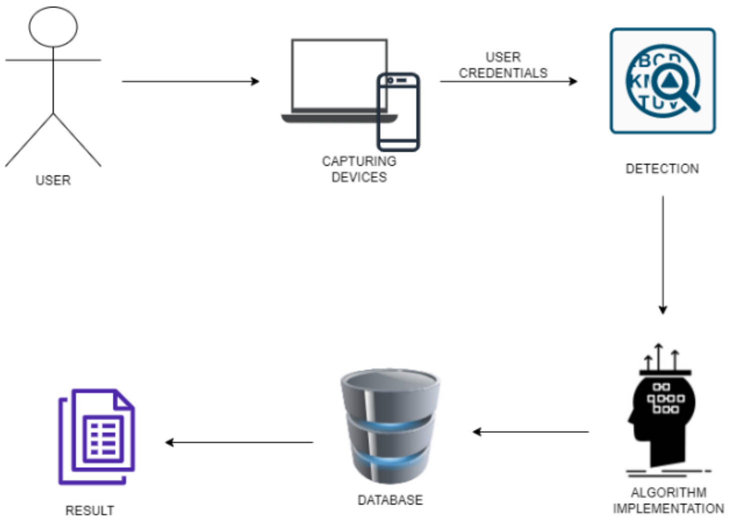
Decryption

The steps in the rounds are simple to reverse because they each contain an opposite that, when used, undoes the modifications. Depending on the key size, each of the 128 blocks is processed via 10 , 12, or 14 rounds. The stages of each round in decryption is as follows :

- Inverse Mix Columns
- Add round key
- Shift Rows
- Inverse Sub Byte

DOI: 10.17148/IJARCCE.2023.125115

The decryption method is the reverse of the encryption procedure, thus I'll explain the processes with notable distinctions.



IV. CONCLUSION

For contributors that upload sensing data, we suggested an end-to-end security solution. This technique enables end-to-end data encryption to safeguard data in transit. All IoT system restrictions are taken into account in the suggested middleware solution. The process is a cyclic process. The sensor readings are first encrypted and hashed using md5 and then sent to the MySQL database. After the encrypted data are decrypted and returned back to the raw value. Then the raw value is hashed using the md5 algorithm and then compared with the previous hashed value for checking the integrity of the data. Then if the integrity returns to be equal to the raw value of the respective cell, it is displayed over to the website, otherwise it's shown as null. This device can be helpful to us in day to day lives and as well it is more secure for the end users too. By implementing this project we can make this as a smart home product for real day to day life temperature and humidity monitoring devices to get quick updates. We can add on some new features like weather forecasting, fire alarm and authentication to make it more secure for all the users. We can also make different devices with the help of this secured algorithm model.

REFERENCES

[1] D. D. Ramlowat.,Binod, Kumar, P., 2019. "Exploring the Internet of Things (IoT) in Education: A Review," Springer Nature Singapore Pte Ltd., pp. 244-254.
[2] Mohammad, Reza, H., &Binod, Kumar, P., 2020. "Security Issues in Internet of Things (IoT): A Comprehensive Review," Springer Nature Singapore Pte Ltd, pp. 354-364.
[3] Mohammad Reza H., Binod, Kumar, P., 2021, "An End-to-End AES Based Cryptographic Authentication Mechanism for Communication on Internet of Things (IoT) Using MQTT" Nat.Volatiles&Essent. Oils.
[4] Reza H., and Binod, Kumar, P., and S. Wedig, 2019. "A Secured Communication Model for IoT," Springer Nature Singapore Pte Ltd, pp.190-196.
[5] Mohammad, A., & Mohamed S., March 2022. IoT Security Using AES Encryption Technology based ESP32 Platform. The International Arab Journal of Information Technology, Vol. 19, No. 2,
[6] Pedro, S., Nam, T., Brandon, C., Behnam, D., &Yuhong, L., 12-15 November 2018. Analyzing the Resource Utilization of AES Encryption on IoT Devices.Proceedings, APSIPA Annual Summit and Conference.
[7] J.GOPIKA, R., ASWATHY, N., 05th April-2014. VLSI Implementation of Cryptographic Algorithms in the Internet of Things. In Consumer Electronics (ICCE), 2018 IEEE International Conference on (pp. 1-5). IEEE.
[8] Irfan, A. L., &Hannan, S., (2018). "4th International Conference on Advances in Electrical, Electronics, Information, Communication, & Bioinformatics (AEEICB-18)".
[9] Shefali, o., and Prof.Vikram, r. International conference on I-SMAC "AES And MD5 Based Secure Authentication In Cloud Computing"