e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

IMPLEMENTING SHA ENCRYPTION ON IOT ARCHITECTURE

Uma.K.Thakur*1, Subham Katre*2, Kartik Singh Negi*3, Kaisangya Mandal*4

*1Assistant Professor, Department of Computer Science and Engineering, PIET, Nagpur (MH), India.

*2Student, Department of Computer Science and Engineering, PIET, Nagpur (MH), India.

*3Student, Department of Computer Science and Engineering, PIET, Nagpur (MH), India.

*4Student, Department of Computer Science and Engineering, PIET, Nagpur (MH), India.

ABSTRACT

In IoT devices, captured plaintext data is sent over the cloud for storing, computing and further processing. But it is a potential concern to secure sensitive information like personal, financial, business, medical, etc. A certain number of researchers established IoT architecture with distinctive layers where data security is solely dependent on cloud service providers (CSPs) which make potential security threats. In this paper, a SHA256 encryption is implemented to support the IoT architecture where the involvement of CSPs for security purposes becomes nullified. As the data become encrypted before it gets sent to the cloud, it becomes more secure and reliable for both the owner and shared users. Additionally, only the IoT node owner and shared users can access those data which provides better security, privacy, and control of data

Keywords: Cloud Service Provider, Encryption, Computing, Data Security, Sha256.

I. INTRODUCTION

The Internet of Things (IoT) is a system of small-connected computational devices, which allows things to connect, collect and transact data, making it capable of directly communicating with computerized systems. So, in the IoT system, it is a potential concern to capture, store, and process all data securely especially for sensitive information like classified, personal, business, medical, financial, etc. sensor produced data is sent to the cloud, Being capable of communicating over network. Therefore, data security entirely depends on cloud service providers (CSPs), they are highly prone to security attacks and securing them is quite challenging. It is very much important to have a secure model for IoT device communication or the way IoT handles the data, so that the data remains secure.

Any kind of data travelling from one place to other needs to be secured nowadays as everyone knows cybercrime has incremented. All the data which any individual shares, accumulates, stores, and exchanges are a paramount asset for the individual as it carries Personal and valuable information and which can be accessed for both good and deplorable purpose. To forefend the data from hacking we are implementing the security system along with the utilization of iot components. The data captured by the iot components will be given to the database and in this process; we are applying encryption on the data to secure it from hacking.

Taking above issue into consideration this research implements sha256 encryption support in IoT architecture. In which data is encrypted first before sending to the cloud from the encryption service enabled IoT node. Moreover, the corresponding IoT node owner and sharer can only access those data.

II. LITERATURE REVIEW

[1] “Database Encryption Scheme'', the paper presents two different coding schemes for databases. Each scheme utilizes the RSA algorithmic rule. The primary one is a field-predicted coding system. All fields square measure accessed by the key of the user. Next, represents record-oriented encryption. It utilizes just one key. This technique applied in subsets and integers teams.

[2] “Confidential data using Python”, the major aim of ubiquitous computing is to provide data anywhere, anytime, anyhow only. It is utilized to enhance the database connections to the Internet. And additionally it should ascertain data confidentiality. Day by day, maleficent attacks and security threats are incremented. an incipient method denominated C-SDA (chip secured data access) is proposed. This controls the users’ access rights and provides data confidentiality. And additionally act as an intermediary between client and encrypted database.

[3] To encrypt data, symmetric key algorithms are utilized. Separate keys are engendered for each connection. All are predicated on next layer protocol. This function can omit a MAC and be used without encryption. A Keyed MAC is utilized to transfer data with message integrity. To encapsulate different higher-level

Protocols, the TLS record protocol are utilized. Next, the TLS Handshake The protocol is utilized to authenticate the client and server. With the rudimental three properties, the connection is established. Asymmetric or public-key encryption algorithms are acclimated to authenticate a peer's identity.

[4] Instead of trusting CSPs, edge encryption can be a better solution in the IoT system where sensitive data is encrypted first before sending to the cloud. Moreover, a user can easily share encrypted node data with other users and only the owner or sharer can access those data which provide better security, privacy, and control of data. Also, this approach can be integrated into the IoT system including smart transportation, precision agriculture, health monitoring, environment monitoring, energy management and many more.

[5] In this paper, an enhanced encryption technique, which combines multiple encryption algorithms, Key Server mechanism is implemented for maintaining Confidentiality, Integrity and Authentication. So that the data being transmitted over internet between different nodes is safe and secure. We are dealing with IoT every day in our life, which makes it very much important to make the communication of such devices secure enough so that no one can tamper the data.

[6] In this paper, we proposed a lightweight encryption model that complies with the limited resources of IoT devices in terms of process and memory. Also, the encryption model also provides a high level of security for the transmitted data through a constant change of the key used for encrypting of transmitted IoT data. In addition, the key size used to encrypt transmitted data in the proposed model is large enough which makes it hard to break by the attackers. The experimental results show outstanding results with an average of 170.7 ms of encryption time for a key size 80 bits where the key size is relatively large and with an average PSNR of 7.7 compared to other algorithms.

III. METHODOLOGY

In this project, we are taking input from hardware IOT sensors i.e. DHT11 (Temperature and sultriness) and Max30100 (Pulse and heart rate) and sending the details to the database for storing the patients' or utilizer's info and hence applying cryptography on it to prevent data hacking or tempering. For this, we are utilizing the SHA256 algorithm. Details about the SHA256 are explicated briefly below.

MAX30100 Sensor:

Max30100 could be a twin sensing element with each the center rate monitor and pulse measuring instrument answer. It's 2 LEDs, a photo detector, optimized optics, and low-noise analog signal process to find pulse oximetry and heart-rate signals.

Fig. 1: Max30100

DHT Sensor:

DHT is a low-cost temperature and sultriness sensor that utilizes circumventing air to calculate sultriness and temperature. Additionally gives a digital signal on pins. It has a diminutive chip integrated for the thermometer.

Fig. 2 DHT11 Sensor

Arduino Uno:

Arduino UNO is a kind of microcontroller that connects all the other IoT components in it. It is like a board that has pins to connect and a built-in led to show its working.

Fig. 3 Arduino UNO

ESP8266:

The ESP8266 could be a cheap Wi-Fi silicon chip, with a full TCP/IP stack and microcontroller capability. To supply net property at an occasional value the unremarkably used contrivance is ESP8266. It’s facile to figure with and utilizer-convivial.

Fig. 4 ESP8266

SHA256 Algorithm:

SHA-256 (Secure Hash Algorithm, FIPS 1822) is one of the cryptographic hash functions which have digest length of 256 bits. It's a keyless hash function, means an MDC (Manipulation Detection Code). In other words, SHA (Secure Hash Algorithm) was developed by the National Institute of Standards & Technology, and further, they came with a new version called SHA-256 (the SHA-2 family), where the number is represented as the hash length in bits.

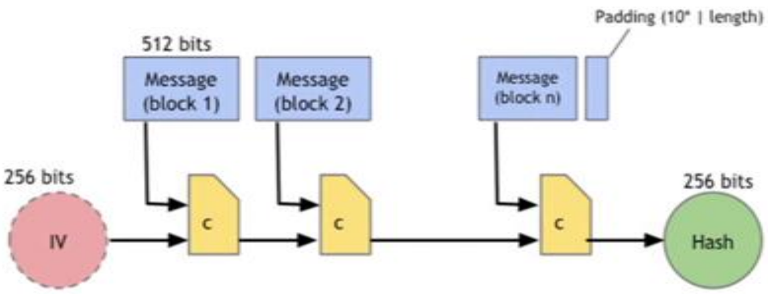

Fig. 5 SHA256 Algorithm Steps

IV. RESULTS

In our proposed model the sensor produced data is encrypted, data is transformed into a secure format that is unreadable unless the recipient has a key. Main goal is to transfer data/commands effectively and efficiently from one end (IoT) to another (User) securely while maintaining the Confidentiality, Integrity, Authentication. It is visible that sender and intended user can only access encrypted data.

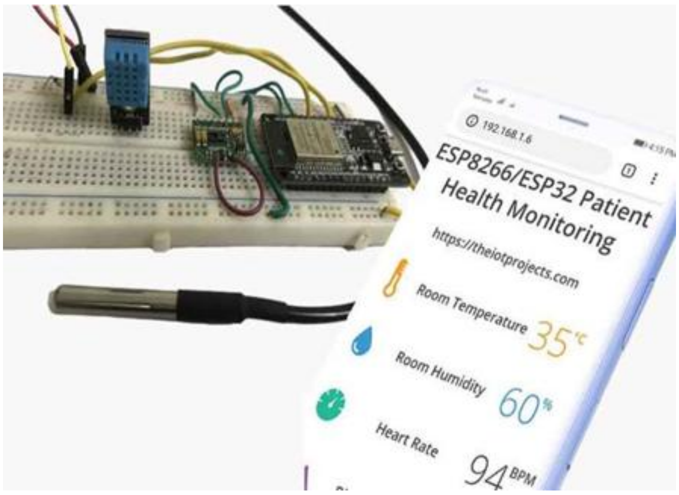

Fig 6: Result Image

V. CONCLUSION

In this paper, we have proposed an encryption method over the data traveling from a hardware contrivance to the software like the database to secure and forefend any information cognate to the company, person, documentation of firms, etc., from hackers utilizing an algorithm.

VI. REFERENCES

[1] Chin-Chen Chang and Chao-Wen Chan, A database record encryption scheme using the RSA public key (Washington, DC, USA), IEEE Computer Society, 2018, p. 345

[2] Luc Bouganim and Philippe Pucheral, Chip-secured data access: confidential data on untrusted servers, VLDB '02: Proceedings of the 28th international conference on Very Large Data Bases, VLDB Endowment, 2020, pp. 131–142

[3] T. Dierks and E. Rescorla, The TLS protocol version 1.2, 2017.

[4] Asif, Md. Rashid Al & Mahfuz, Nagib & Momin, Md & Hossain, Md. Alam & Roy, Saumendu. (2019). Prototype Implementation of Edge Encryption in IoT Architecture. 10.1109/ICCCNT45670.2019.8944810.

[5] Rupesh Bhandari, Kirubanand V B "Enhanced encryption technique for secure iot data transmission" International Journal of Electrical and Computer Engineering (IJECE) Vol. 9, No. 5, October 2019, pp. 3732~3738 ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp3732-3738

[6] Mohammed Abbas Fadhil Al-Husainy , Bassam Al-Shargabi "Secure and Lightweight Encryption Model for IoT Surveillance Camera"https://doi.org/10.30534/ijatcse/2020/143922020.