Grenze International Journal of Engineering and Technology, June Issue

Lightweight Symmetric Encryption Scheme for Public Healthcare Clouds

Ravi V[1] and Dr. Poornima A.S[2]
[1-2]Department of Computer Science Engineering, Siddaganga Institute of Technology, Tumakuru, India
Email: ravi@sit.ac.in, aspoornima@sit.ac.in

***Abstract*—Due to the pandemic and other health-related issues, Healthcare data of individuals are rising day by day on public clouds which can be easily compromised by cloud administrators, cloud operators, and insurance company individuals. It is highly required to keep these data confidential and allow access to individuals with credentials. Data from body sensors help to capture the real health conditions in plain formats which can be sensible and can be misused by the insurance companies, hospital members for making fraud transactions and violating the health insurance norms. In this regard, the proposed method can be used to enhance the confidentiality of the sensed data using the Fernet Encryption scheme which uses a 128 Bit AES encryption scheme with CBC mode and padding enables encryption for confidentiality and HMAC with these configurations to help us authenticate the user. Healthcare data such as Patient ID Proof, Patient Personal data, Health records are more vital and need to be accessed securely. In the proposed model, encrypted Health records of patients are stored and accessible by authorized persons who are shared with keys with less processing time, and the proposed scheme is extended for encryption and decryption of a large database of patient data to suit the Big Data Healthcare domain. The proposed method also ensures data is accessible to authorized users and avoids insurance fraud and other data leakage problems.**

***Index Terms*— Big data , Healthcare, Fernet Encryption, Two level encryption.**

I. INTRODUCTION

Recent pandemic attacks [1], [2] on healthcare data stored in private and public clouds raise concerns on confidentiality and authentication issues in accessing the information by the cloud operators, hospital members, insurance company professionals. Most of the data servers store the patient records in an unencrypted format identified by a unique ID which can be easily compromised to generate fake claims in insurance companies, frauds at hospitals by blocking the hospital resources using the compromised patient data. These issues raise the concern for encrypting the data at data servers and allowing only authorized users to operate on the data using authentication schemes.

Figure 1. show the flow of information among hospitals and insurance companies, where patient details are accessed from insurance agencies and other third party agencies to verify the claims and these require credentials to be needed to the right person for claims. The software used by hospital management to store and retrieve the patient data supports password based authentication which can be compromised and data can be misused during these claims, by using Biometric based data access system [3] proposed by *Shakil et.al*., can ensure data is accessible to right user at right time.

Grenze ID: 01.GIJET.8.2.509

IoT sensors which are deployed near or on the patients can extract health conditions from the patients in the plain text formats which are recorded on the local servers for diagnosis purposes, extracted data will be accessed by the physicians to diagnose and prescribe the medications to the patients. IoT technology face with challenges in data encryption and decryption where sensors are light weight and can perform encryption using light weight encryption techniques and also need secure communication with the local servers through the use of protocols such as CoAP [4], MQTT [5], LwM2M[6], AMQP[7] protocols which enable sensor data to be stored on cloud data centers by pulling the data from the sensors and accumulating those in the data centers. IoT sensor uses 6LoWPSec which is an extension given to the 6LoWPAN protocol which supports ciphering of data and deciphering at the cloud side, enabling end to end encryption in IoT [8] is expensive operation and requires additional operations to be carried out at both nodes and cloud level.

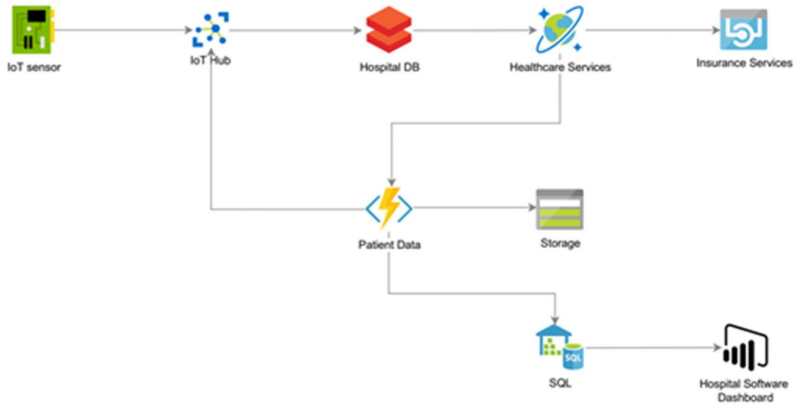

Figure 1. Hospital database and Healthcare service accessed by third party agencies

The need for Bio-metric based authentication, End-to-End encryption, Authentication schemes rises the requirements of security in Healthcare IoT environment, with these requirements the proposed model provides low-cost solution to IoT user authentication using Bio-metric based access schemes, a Two-level security scheme for data encryption at sensor nodes, and End-to-End encryption for data confidentiality.
In this paper, we discuss the related works carried out in Healthcare data breaches and limitations of the existing solutions proposed. Thereafter, proposed model is described in the next subsequent sections followed by implementation and results of the proposed model. Lastly, we offer conclusions and highlight the future directions.

II. Related work

Kashish A et.al [3] et.al have proposed the biometric based authentication for various users of Health care services ranging from ordinary to VIP staff of hospital management system. The author explains the use of signature based authentication for each user who have enrolled for health care services. Model records the signatures of each user and authenticate as and when user tries to access a Health Cloud service. System allows authentication of users but confidentiality of data is still a limitation since data is stored in plain text format.
Karim Abouelmehdi et.al [9] have surveyed the requirement of Big-data in the field of Healthcare and importance of the data privacy and its impact on Health care services are elaborated. The author also explains how Big-data security lifecycle highlights three important requirements such as data security, access control, and information security for any data center. Health care services need to support privacy-preserving data access to the patient data and also enable anonymous data access which is difficult to achieve in hospital software and third-party software in which data is accessed by hospital agents and insurance agents for claims. Author also explains the privacy preserving data access through De-identification, Hybrid execution model, Identity based anonymization techniques for big data processing.
Sarada Prasad et.al [10] proposed a distributed key management scheme for IoT technology where keys are shared among the IoT sensors and cryptographic process is shared to a local entity which in-turn communicates with cloud entities for secured data communication. The authentication is a decentralized approach where a mobile agent is deployed to authenticate the nodes and also allow communication among nodes securely. Again confidentiality of the patient data is needed since data are stored on cloud data centers which need to be accessible to only authorized users.

Kedir Mamo Besher [11] proposed a cryptographic scheme to allow data sensed by the IoT sensors to be encrypted using two level encryption scheme where data is encrypted at sensor node and then stored in the cloud data servers which are later accessed with agents (Doctors) with whom keys are shared to decrypt the patient data and prescribe the medication for the patient. Data generated by the sensor nodes are transformed to ASCII/Binary and then encrypted using the keys {key1, key2} which are shared among the Doctors who can later allow decryption on same cipher information using the keys. Usage of multiple keys for encryption and decryption process will result in extra overhead for overall system.
Farha Nausheen [12] surveyed various vulnerabilities in Healthcare solutions and also proposed the schemes such as Code obfuscation, Check summing, Return oriented programming, Key protection and access control schemes, Anomaly detection, for remote health data access in cloud service. Each of the method proposed enables confidentiality and authenticated access to the Healthcare services using various schemes

III. MOTIVATION

Healthcare data needs to be protected against unauthorized access and using Biometric based solutions may lead to expensive deployment of model. Light weight encryption schemes such as Fernet encryption can be extended to encrypt the IoT device sensed data which are plain text and smaller in size using a pair of keys which can ensure two level encryption to protect against data leak and data frauds.

IV. PROPOSED DESIGN

Figure 2. shows the proposed model of Healthcare services which are provided to third party agencies in a secured way through API services which limits the access of Patient data from the Hospital database service. Firebase provides an easy way to access the stored information through API service which also enables constrained access to the patient database. Following are the various phases of the proposed system.

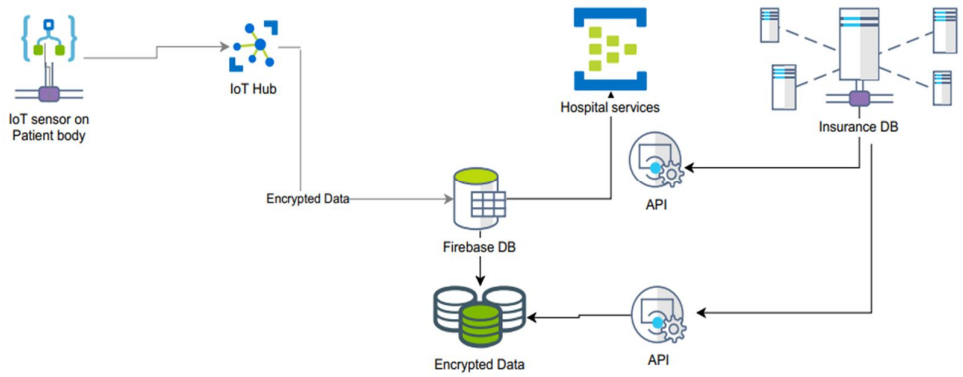

Figure 2. Proposed system

A. Data acquisition from sensor nodes

Sensor nodes deployed on the patient body acquires data in plain text format which can read through the serial communication as shown in Figure 4. In the proposed model, DHT11 sensor which is used to sense the temperature of a patient and read through the serial communication to record the patient data in a Firebase database in encrypted format. The proposed model ensures data is accessible to authorized users only so using the Fernet encryption scheme where data is encrypted and stored on the Firebase database. Patient data need to be made available only to the doctors who are medicating the patients, the proposed model generates a fixed size key for each doctor using the doctor personal information such as Doctor ID or unique identification since these ID are unique and reliable, data encryption key and decryption can be obtained from these identification numbers. For e.g. the doctor ID can be given as follows

TABLE I. DOCTOR ID AND BASE64 ENCODING FOR FERNET KEY GENERATION LOGIC

Unique ID of Doctor	Base64 coding of ID
7123	NzEyMw==

The Unique ID of the doctor can be generated using Base64 encoding scheme to generate a unique key for each doctor and can be used in Fernet encryption scheme for encryption of plain text sensed data on Firebase Database which are shared among Doctors who can give the same Unique ID as a key for decryption as shown in Table 1. can be used for encryption and decryption as shown in Figure 3.

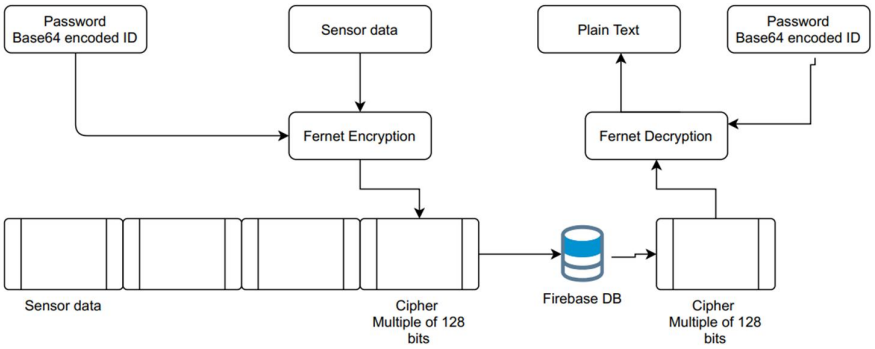

Figure 3. Encryption and Decryption of sensor data

Combination of Base64 encoding scheme and Fernet encryption scheme is used in the proposed system where Base64 encoding helps to keep the sensed data intact and provide integrity where as Fernet encryption enable confidentiality to allow access sensed data only to Doctors and authorized person who need the credentials which can be shared by means of key sharing schemes.

V. RESULTS

The proposed system is implemented using python language with Firebase Database as backend database for storing the sensor data obtained from DHT11 sensor (as shown in Figure 4.) which senses the data from the body and obtained in the serial communication terminal which is configured and programmed using Arduino programming. The sensed data has to be encrypted using the Fernet encryption scheme with Base64 encoded string of doctor ID which is unique for each doctor and cannot be forged by the attackers.

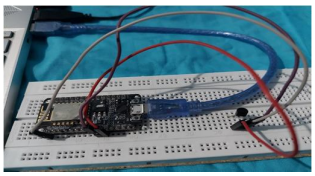

Figure 4. DHT11 Sensor to Sense Data from the Body

Figure 5. Figure 6. and Figure 7. shows the project execution and database configurations done in google firebase database setup using the firebase_admin_module( ) which allows admin to configure the database and storage bucket associated with the database.

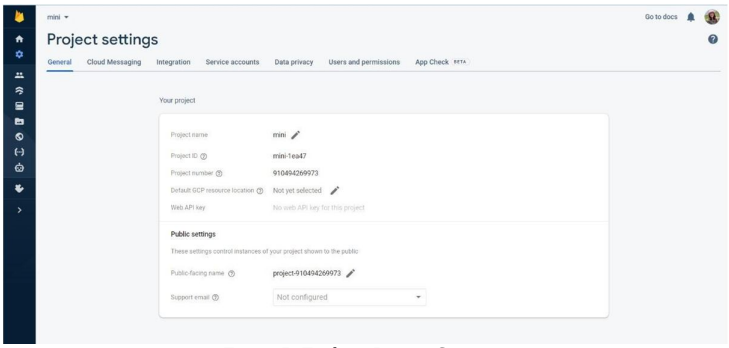

Figure 5. Firebase Project Settings

Figure 6. shows the data from the sensor nodes are encrypted using the Ferent encryption scheme and stored in the google firebase server which can be later used by the Doctors by decrypting with the Doctor ID.

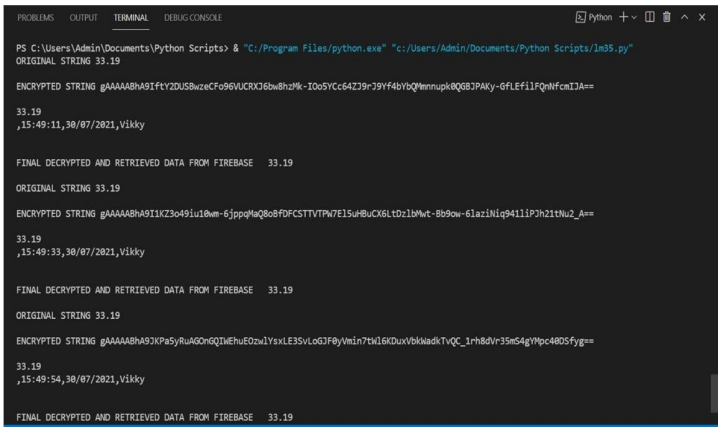

Figure 6. Python script to extract sensed data and Fernet Encryption

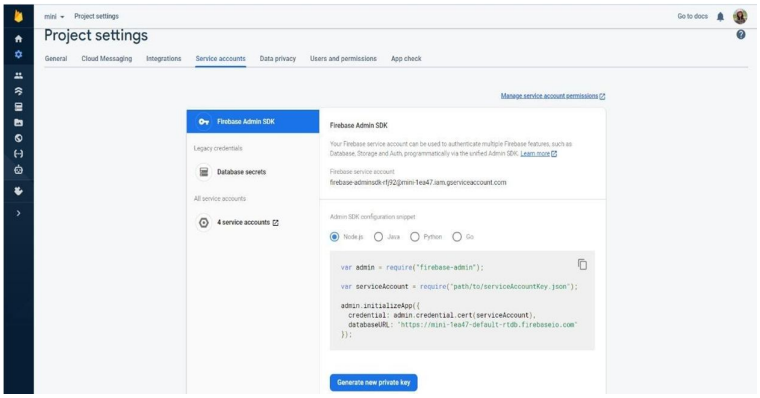

Figure 7. Project Database setup

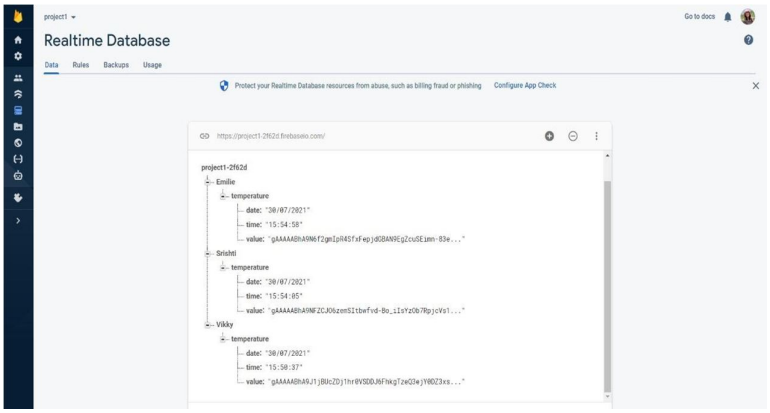

Figure 8. Real-time database on Firebase

VI. CONCLUSION

The proposed model encrypts the sensor data at the nodes using a lightweight symmetric scheme such as the Fernet encryption scheme best suited for the IoT environment to encrypt the patient health data sensed by the sensor nodes. The use of Fernet encryption can also improve the bootstrapping of encryption schemes at sensor

nodes which in turn help to IoT environment to support confidentiality and authentication to end-users. The use of Google Firebase as the database for healthcare also enables secure data transfer among hospital and insurance agents using API service. The model can be improved by building distributed environments such as Blockchains and allowing transparent communication among hospitals and insurance agencies.

REFERENCES

[1] The biggest healthcare data breaches of 2021," *Healthcare IT News*, Nov. 16, 2021. https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021 (accessed Jan. 06, 2022).

[2] O. C. Kurian, "Data, Privacy, Pandemic: India just had the Biggest Medical Records Breach Ever," *ORF*. https://www.orfonline.org/expert-speak/data-privacy-pandemic-india-just-had-the-biggest-medical-records-breach-ever/ (accessed Jan. 06, 2022).

[3] K. A. Shakil, F. J. Zareen, M. Alam, and S. Jabin, "BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 32, no. 1, pp. 57–64, Jan. 2020, doi: 10.1016/j.jksuci.2017.07.001.

[4] CoAP - Constrained Application Protocol, *Radiocrafts*. https://radiocrafts.com/technologies/coap-constrained-application-protocol/ (accessed Jan. 09, 2022).

[5] MQTT - The Standard for IoT Messaging. https://mqtt.org/ (accessed Jan. 24, 2022).

[6] LwM2M — Lightweight M2M standard — protocol and its benefits. https://www.avsystem.com/blog/lightweight-m2m-lwm2m-overview/ (accessed Jan. 24, 2022).

[7] "Home | AMQP." https://www.amqp.org/ (accessed Jan. 24, 2022).

[8] G. Glissa and A. Meddeb, "6LowPSec: An end-to-end security protocol for 6LoWPAN, *Ad Hoc Netw.*, vol. 82, pp. 100–112, Jan. 2019, doi: 10.1016/j.adhoc.2018.01.013.

[9] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," *J. Big Data*, vol. 5, no. 1, p. 1, Jan. 2018, doi: 10.1186/s40537-017-0110-7.

[10] S. Gochhayat *et al.*, "Reliable and secure data transfer in IoT networks," *Wirel. Netw.*, vol. 26, Nov. 2020, doi: 10.1007/s11276-019-02036-0.

[11] IoT Sensor Initiated Healthcare Data Security | IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9154453 (accessed Jan. 09, 2022).

[12] F. Nausheen and S. H. Begum, "Healthcare IoT: Benefits, vulnerabilities and solutions," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, Jan. 2018, pp. 517–522. doi: 10.1109/ICISC.2018.8399126.