ANNA - A UNIFIED FRAMEWORK FOR DATA SECURITY IN HEALTHCARE INTERNET OF THINGS

R. Shantha Mary Joshitta and L. Arockiam
Department of Computer Science, St. Joseph's College (Autonomous), India

Abstract

Today, the cyber-physical interactions are made possible with the development of internet and smart technologies. Smart objects such as sensors, RFID tags and actuators are the building blocks of such pervasive network, called as Internet of Things (IoT). IoT has a good number of real time applications in all domains including medical industry. It has great impact on modern healthcare with promising economic, technological and social benefits. Researchers across the globe already have started to explore a variety of technological solutions to enhance healthcare system by incorporating the potential of the IoT. This paper presents a unified framework ANNA, for integrating IoT in healthcare system. It presents three lightweight algorithms to enhance data security in the smart healthcare environment. In addition, this paper provides a detailed working scenario which would be helpful in implementing smart healthcare units in rural India. The working scenario of the ANNA smart healthcare system and the workflow of the framework are also elaborated in this paper. The proposed framework is proved against possible attacks in the healthcare environment. The salient features of the framework are outlined and this research creates a hope that the smart healthcare units based on ANNA framework will offer on time medical care to the needy and the downtrodden.

Keywords:

ANNA, Internet of Things, Data Security, SAT_Jo, JAC_Jo, AroSheb_Jo, Healthcare, Medical Service

1. INTRODUCTION

Over the last few years, lightweight wearable sensor nodes and objects are connected directly with each other. They are empowered to capture and share vital data of their own without human intervention. This convincing forward technology is called as Internet of Things (IoT). IoT enabling solutions spur the advent of many novel and fascinating applications. Among others, smart cities, smart grids and smart healthcare are some of the leading real time applications. In the wake of this evolutionary trend, a collection of sensing devices and objects are used in the healthcare sector for non-invasive monitoring of various healthcare data of the patients. It promises to improve access to healthcare services to everyone at any time, provide state-of-the-art medical care even to remote locations, offers preventive care, allows prompt diagnosis of acute complications and reduces the cost of the healthcare services [1] affordable to the poor and the deserved. Many a time, sensor nodes are employed in medical scenario to collect the comprehensive physiological information of the patients and store it in the cloud servers and then send the stored data wirelessly to the medical staff for further analysis and review. Advances in the design of IoT technologies allow these sensor devices to be smart in collecting, recording and analysing stream data faster and more accurately. Staying true to this IoT vision, this research proposes a framework ANNA for secure accumulation and usage of the patient medical information by enhancing the authentication and confidentiality of data collected in the healthcare system.

1.1 NEED FOR IOT IN HEALTHCARE DOMAIN

Today, the demand for connected devices in industries such as energy, automotive and consumer spaces that can report or react to certain condition keeps on increasing. These networks of smart devices provide a new level of convenience, efficiency and automation. On the other hand, the prevalence of chronic diseases across the world urges to find new ways to improve patient outcomes, increase access to care and reduce the cost of medical care [2]. This creates an opening for smart devices not only to track vital health information of the patients, but also for lessening the need for direct patient-physician interactions. In healthcare sector, the Internet-connected devices have been introduced in various forms such as fatal monitors, electrocardiograms, temperature and blood glucose level monitors. The advancements in sensor technology, the ubiquitous availability of 3G and 4G cellular technologies and dropping costs of communication devices are creating opportunity for integrating IoT in medical care [3]. Moreover, using seamless, continuous remote patient health monitoring, healthcare providers, insurance payers and governments are looking for significant ways of providing care to the patients, while reducing cost of the medical services [4]. So, the next generation is blissful to see a revolution in treatment and diagnosis of disease using smart devices and objects.

2. RELATED RESEARCH WORKS

Aamir Hussain et al. [5] proposed a people-centric IoT healthcare framework for the elderly and disabled people. The proposed framework provided a service oriented emergency response at abnormal health condition. The researchers concentrated on context manipulation from the mobile device for emergency situation and modeling mobile context sources as services. The medical resources were efficiently used to provide real-time medical services in case of emergency. The research was evaluated for its efficiency and cost effectiveness. The author in [6] described a healthcare monitoring system developed using the loT and RFID tags. The researcher experimented and proved the impact of IoT enabled healthcare at medical emergencies. Various evaluation results, supervising and weighing the health status of the patient with loT devices were also presented. Vikas Vippalapalli et al. [7] designed and implemented a smart health monitoring system. Lightweight wearable sensor nodes were used to monitor patient real time sensing data and analysis medical parameters of the patient. The proposed research aimed at making the healthcare accessible for all the people and offering patient-center medical care. It focused on preventing the delays in arrival of the medical information of the patients from accident spot or in emergency situations and reducing manual data entry for patients' data. A tele-monitoring application was presented in this paper and concentrated in collecting medical information from a patient. In [8], Prosanta Gope et al. highlighted the security requirements in Body Sensor Networks (BSN)-based modern healthcare system. The researchers proposed a secure IoT-based healthcare system using BSN, called BSN-Care, for handling security issues efficiently. The authors modelled a BSN-Care to achieve the security properties and the analytical results were also presented. Natarajan et al., [9] proposed a Health-IoT Platform Based model and achieved machine to machine communication for healthcare data. The authors integrated Intelligent Medicine Box, Intelligent Packaging, Unobtrusive Bio-Sensor and RFID Technology for IoT-Based Personal Healthcare in Smart Spaces. An intelligent home-based platform was proposed and implemented. An intelligent medicine box based on open-platform (iMedBox) was presented and inter-changeability for the integration of devices and services. Wearable sensors and intelligent medicine packages with in-home healthcare services were also proposed for improved user experience and service efficiency. Kritika et al. [10] reviewed the authentication based security model for IoT. The authors proved the incapability of several existing authentication schemes in securing the IoT. The authors explained the weakness of XOR manipulation in encryption schemes such as AES and Blowfish. The XOR operation had the reversal tendency of retrieving the passwords from the manipulation code created using XOR. So, the authors had proposed another robust method for secure authentication scheme. In [11], Byung Mun Lee proposed an open healthcare platform structure design and suggested an authenticated registration process. The proposed platform linked a mobile device with convenient registration and shared diverse types of medical devices and services. Furthermore, the authors introduced and implemented an IoT based healthcare mobile application for verifying the efficiency of the proposed method. The above said research contributed a user authentication and platform development for IoT-based medical devices. Patrick Lacharme et al. [12] proposed a new protocol by combining protected biometric data and a classical synchronous one time password. It enhanced the security of user authentication while preserving usability and privacy. It proposed the generalization of the synchronous one time passwords by adding a biometric feature. Bio-hashing algorithm was used in the protocol and experiments were carried out on a homemade benchmark dataset.

3. OBJECTIVES

Security is one of the most prominent bottlenecks in the realization of IoT and extremely challenging due to the nature of the IoT environment. To gain trust of the people on IoT, the application models must support application development with security and privacy protection. As the variety and growing number of connected devices are introduced into IoT, potential security risk escalates. Real time IoT applications generate massive amounts of personal data from healthcare, household and financial transaction of many business enterprises. Lack of security and privacy will cause struggle in the adoption of IoT in such business firms and individuals. Security challenges may be resolved by strengthening the confidentiality and authentication of IoT devices and users. This research focuses on incorporating IoT in healthcare domain for enhancing the provision of patient centred medical care. But, ensuring the efficiency and accuracy of the data accumulated and generated by the IoT devices are the most challenging issue in healthcare services [13]. So, the primary objective of this paper is to design a framework for secure IoT enabled smart healthcare system by enhancing authentication of the users and smart medical devices of the system [20].

4. WORKING SCENARIO OF ANNA SMART HEALTHCARE SYSTEM

The working scenario of the proposed ANNA Smart Healthcare System is presented in Fig.1. It has three phases namely, Medical Data Acquisition phase, Medical Data Storage phase and Medical Data Application phase.

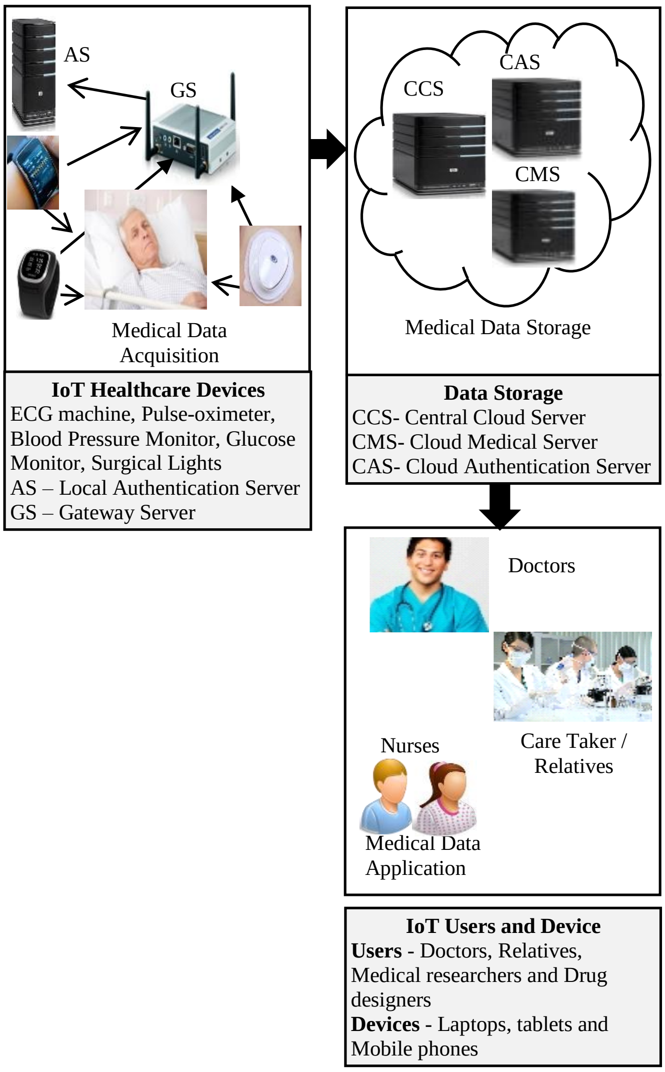
AS
GS
Medical Data Acquisition
IoT Healthcare Devices
ECG machine, Pulse-oximeter, Blood Pressure Monitor, Glucose Monitor, Surgical Lights
AS – Local Authentication Server
GS – Gateway Server
CCS
CAS
CMS
Medical Data Storage
Data Storage
CCS- Central Cloud Server
CMS- Cloud Medical Server
CAS- Cloud Authentication Server
Doctors
Nurses
Care Taker / Relatives
Medical Data Application
IoT Users and Device
Users - Doctors, Relatives, Medical researchers and Drug designers
Devices - Laptops, tablets and Mobile phones

Fig.1. Working Scenario of the ANNA Smart Healthcare System

4.1 MEDICAL DATA ACQUISITION PHASE

The medical information from the patients such as Blood Pressure, Blood Oxygen, Heart Rate, No. of Steps Walked, Distance Walked, Calories Burned, Sleep Hour, Sleep Quality and Blood Glucose along with the date and time are collected in this phase. The smart medical devices such as sensors, pulse-oximeter, surgical lights, blood pressure monitor, glucose monitor and so on are used for collecting medical information and communicate it to the nearest Gateway Server.

4.2 MEDICAL DATA STORAGE PHASE

The collected medical information is encrypted at the Gateway Server or local Authentication Server using the lightweight block cipher *JAC_Jo* and saved in the Cloud Medical Server (CMS).

4.3 MEDICAL DATA APPLICATION PHASE

The stored medical data are used by the medical users such as doctors and nurses concerned, relatives of the patient, medical researchers, drug designers and medical insurance providers. The users can access the medical data by proving their authenticity using the OTP generated by the Cloud Authentication Server (CAS). The CAS generates the OTP using *AroSheb_Jo* OTP generation algorithm and sends it to the users' registered devices. If the user fails to resubmit the OTP within time, he is not permitted to access the medical data.

5. THE PROPOSED FRAMEWORK

The ANNA framework for healthcare IoT environment is depicted in Fig.2. The proposed framework consists of three lightweight algorithms namely, *SAT_Jo*, *JAC_Jo* and *AroSheb_Jo*. Before using these algorithms, any user or device has to register with the ANNA framework. The registration process and methodology of the proposed algorithms are elaborated in this section.

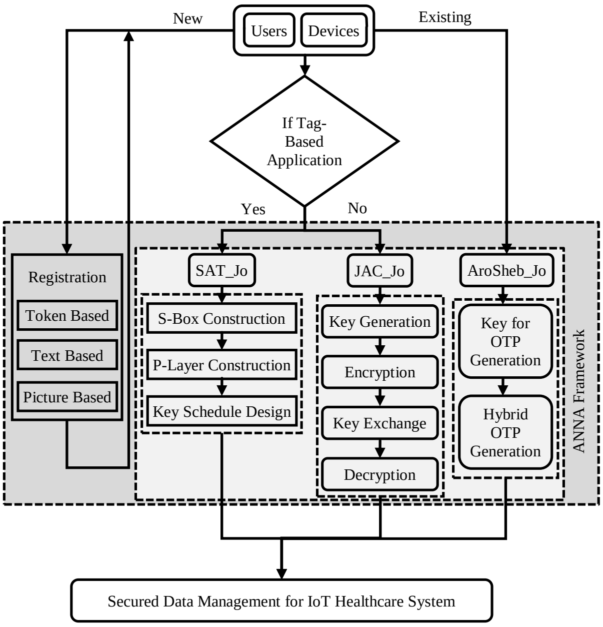

Fig.2. The ANNA Framework

5.1 REGISTRATION PROCESS

It is a one-time process, normally carried out by the Authentication Server (AS). Registration of Patients, Medical Devices and User devices are carried out in this process. The medical devices are the smart devices used to accumulate medical information from the patients and the user devices are the digital gadgets such as Laptop, Desktop and Smart phones used by the medical users [14].

5.2 TEXT BASED REGISTRATION

Any Patient of the healthcare system needs to be registered using this registration process as presented in Fig.3.

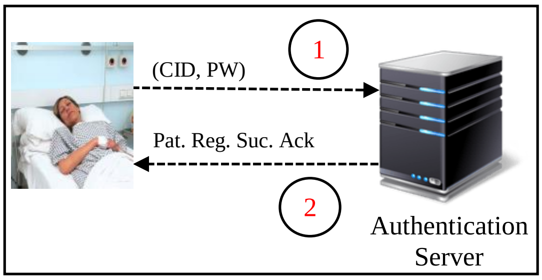

Fig.3. The Patient Registration Process

The Citizen Identification Number (CID), a proposed unique identification number for every human and a password are collected from the Patients. The hash function is applied on them to generate a secret User Authentication Code (*UAuth_Code*). These details are stored in the *Pat_Reg_Tab* of the IoT Gateway Server (*GS*) and the Authentication Server (*AS*) for further references. The content of the *Pat_Reg_Tab* is presented in Table.1.

Table.1. Patient Registration Table.(Pat_Reg_Tab)

CID_1	PW_1	PID_1
CID_2	PW_2	PID_2
CID_3	PW_3	PID_3
...	...	...
...	...	...
...	...	...
CID_n	PW_n	PID_n

5.3 TOKEN BASED REGISTRATION

Resource constrained devices are registered using token based registration process. The resource constrained devices are devices used for measuring medical parameters such as body temperature, respiration, heart rate, body weight, skin conductance, galvanic response, blood glucose level, muscle contraction, motion analysis and so on. They are registered using this process which is described in Fig.4.

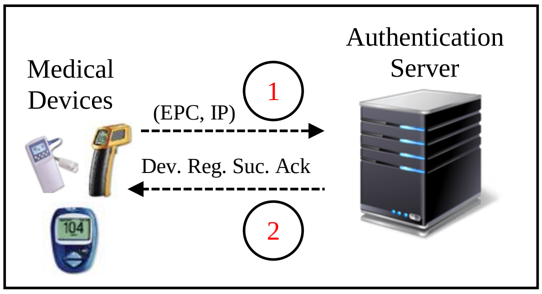

Fig.4. The Medical Device Registration Process

Electronic Product code (EPC) and IP address of the devices are collected and generated a unique id for the medical device called as Device Identification Number (DID). These details are saved in the Medical Device Registration Table, *MD_Reg_Tab* that is presented in Table.2.

Table.2. Medical Device Registration Table.(*MD_Reg_Tab*)

UID_1	UIP_{11}	UIP_{12}	UIP_{13}	...	...	UIP_{1n}
UID_2	UIP_{21}	UIP_{22}	UIP_{23}	...	...	UIP_{2n}
UID_3	UIP_{31}	UIP_{32}	UIP_{33}	...	...	UIP_{3n}
...	...	...	...	...	...	...
...	...	...	...	...	...	...
UID_n	UIP_{n1}	UIP_{n2}	UIP_{n3}	...	...	UIP_{nn}

5.4 PICTURE BASED REGISTRATION

Resourceful devices i.e. user devices use this picture based registration process. Details such as CID, password, mail address, mobile number, EPC and IP are collected from the users for registration. A set of system generated patterns is displayed for the user selection. Selected patterns along with the other details are saved in the *User_Pattern_Tab* and *UD_Reg_Tab* respectively. The steps involved in this kind of registration are depicted in Fig.5.

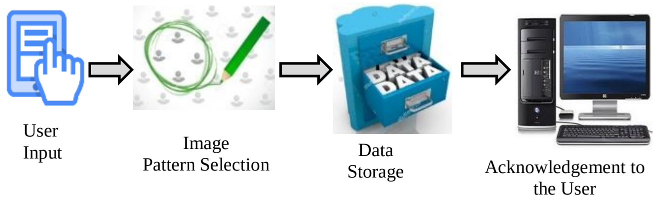

Fig.5. The User Device Registration Process

The *User_Reg_Tab* and the *User_Pattern_Tab* are presented in Table.3 and Table.4 respectively.

Table.3. *User_Reg_Tab*

CID_1	PW_1	$Mail\_id_1$	$Mble\_no_1$	UID_1
CID_2	PW_2	$Mail\_id_2$	$Mble\_no_2$	UID_2
CID_3	PW_3	$Mail\_id_3$	$Mble\_no_3$	UID_3
..	..	..	..	..
CID_n	PW_n	$Mail\_id_n$	$Mble\_no_n$	UID_n

Table.4. User_Pattern_Tab

EPC_1	IP_1	DID_1
EPC_2	IP_2	DID_2
EPC_3	IP_3	DID_3
..	..	..
..	..	..
EPC_n	IP_n	DID_n

The algorithm *ANNA_Reg* is given below.

```
Algorithm ANNA_Reg

Input: Citizen Identification Number (CID), User Password
       (pw), Electronic Product Code (EPC), IP Address (IP),
       Employee ID of the User (EID), User Device Id (DID),
       User Password (pwd), Mail_id (mail_id) and Mobile no
       (mble_no)
Output: Secret Patient Id (PID), Device Id (DID), Secret User Id
        (UID)

BEGIN
Step 1: Read Type of Registration
Step 2: If Type == 'U' then // User Registration - At AS/GS
        Read CID, pw
        $PID = \mathbf{H}(CID \oplus pw)$
        $User\_Reg\_Tab \leftarrow CID, pw, PID$ // in User Registration Table
        return (ack) //Sends Acknowledgement to the User

        Else if Type == 'RCD' then //Resource Constrained
        Read EPC, IP Devices Registration - At AS/GS
        $MD\_Id = \mathbf{H}(IP \,||\, EPC)$
        $MD\_Reg\_Tab \leftarrow EPC, IP, MD\_id$ // Stored in Device Registration Table
        return (ack) // Sends Acknowledgement

        Else // Resourceful User Devices Registration - In CAS
        Read EID, pwd, DID, mail_id, mble_no
        $MEID = EID||DID$;
        // CAS displays a set of random image patterns and User selects his choice
        $User\_Reg\_Tab \leftarrow EID, pwd, mail\_id, mble\_no, DID,$ UID and MEID
        $User\_Pattern\_Tab \leftarrow$ Pattern selected and MEID
        return (ack) // Sends Acknowledgement
        End if
Step 3. Login () //Login process
END
```

The flow diagram of the *ANNA_Reg* algorithm is presented in Fig.6.

After completing the registration process, the patients are mapped with medical devices and medical staff. It is helpful to track whose medical data is to be collected by a particular medical device and who are accessing the medical information of a patient. The mapping process is performed by the Authentication Server. After mapping only, the data storage and data usages are possible. This mapping information is stored in the *Pat_DR_Tab*. In the *Pat_DR_Tab*, '1' represents 'Authenticated User' and '0' represents 'Non-Authenticated User'. It is helpful to understand the number of medical devices connected to a particular patient. Any user can view the medical data but not permitted to modify it. The format of the *Pat_DR_Tab* is presented in Table.5.

Table.5. Content of *Pat_DR_Tab*

	UID_1	UID_2	UID_3	--	--	UID_n
PID_1	1	1	0	--	--	1
PID_2	0	0	1	--	--	0
PID_3	1	0	1	--	--	0
--	--	--	--	--	--	--
--	--	--	--	--	--	--
PID_n	1	0	1	--	--	1

SAT_Jo encrypts the medical data using SPN structure and stores it in the GS if it is collected from the resource constrained devices. *JAC_Jo* is designed using Feistel structure to perform encryption and decryption operations. It is used to send data securely from a high end device spectrum which is resourceful but supports lightweight algorithms in order to interoperate with the constrained sensors. *AroSheb_Jo* offers an OTP for the user device for accessing the medical data from the CMS. Algorithm *SAT_Jo*: This algorithm constructs a 4×4 S-Box based on the finite field GF (24), the Galois field of order 24 [14]. It offers a P-Layer and key schedule for encrypting medical data where only encryption is required. It runs in the low end device spectrum. This algorithm runs in the GS by which the medical devices are networked with user devices. Algorithm *JAC_Jo*: This algorithm is designed using Feistel structure. It runs in the high end device spectrum but aggregating data from the low end devices. This algorithm offers encrypting and decryption of data by which security is enhanced [15]. This secure block cipher encrypts the data before sending it to the server and decrypts it at the user device. It runs in the *GS*/*LS* as well as in the user devices to encrypt and decrypt the medical data [16]. Algorithm *AroSheb_Jo*: It uses OTP technique to authenticate the resourceful devices used by the users of the healthcare IoT system [17]. This algorithm runs in the CAS and generates an OTP for authenticating the user device. If the user resubmits the OTP within the stipulated time, it authenticates the device to access the data from the server. Otherwise, it blocks that particular user device. The sequence of operations of the proposed ANNA Framework is presented in Fig.7.

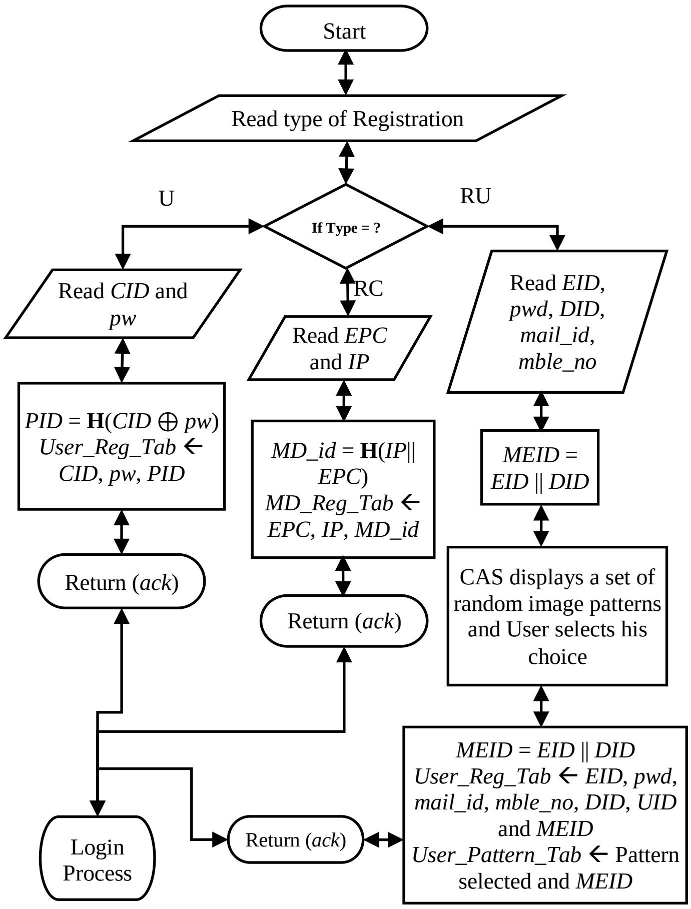
Start
Read type of Registration
U
RU
If Type = ?
RC
Read CID and pw
Read EPC and IP
Read EID, pwd, DID, mail_id, mble_no
PID = H(CID ⊕ pw) User_Reg_Tab ← CID, pw, PID
MD_id = H(IP|| EPC) MD_Reg_Tab ← EPC, IP, MD_id
MEID = EID || DID
Return (ack)
Return (ack)
CAS displays a set of random image patterns and User selects his choice
MEID = EID || DID User_Reg_Tab ← EID, pwd, mail_id, mble_no, DID, UID and MEID User_Pattern_Tab ← Pattern selected and MEID
Login Process
Return (ack)

Fig.6. Flow Diagram of *ANNA_Reg* Algorithm

6. SECURITY ANALYSIS OF THE ANNA FRAMEWORK

A test bed for ANNA framework is created and medical data are collected for evaluation. It is experimented in a Senior Citizens Care Home where three patients of age more than 60 are selected for analysis. An experimental set up is created using RCE - Wh10 - Smart fitness Band Tracker a Smart watch with Pedometer, Lenovo ThinkPad X250, Moto G5s Plus and a BSNL DSL W200 Modem. Patients are asked to wear the smart watch for a period of six months from December 2017 to May 2018. Blood Pressure (BP), Blood Oxygen level (Spo$_2$) and heart rate are collected daily twice and collected data are stored in a Laptop. The medical data are collected daily after 9 am and 6 pm to keep them under continuous medical surveillance. The medical staff carefully observed them by viewing the patients' medical data in his mobile and any change in the data is found by the doctor and immediate action is carried out. The collected data are transferred to the *LS* i.e. a laptop. *LS* applied *SAT_Jo* lightweight block cipher to encrypt the collected medical data and saved it in the Google Drive, freely available cloud storage. The medical team which has access to these medical data view these data by proving their authenticity. The details of the data collected by the ANNA framework are presented in Table.6. The sample medical data are listed in Table.7.

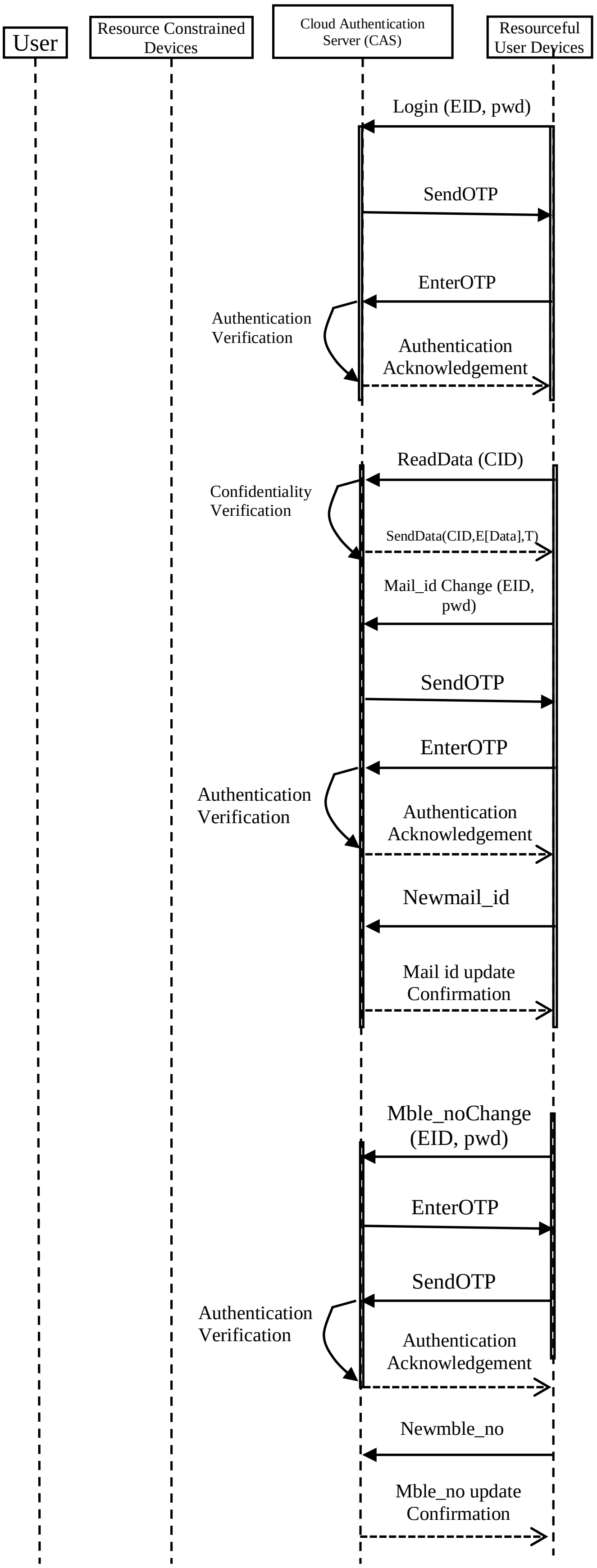
User
Resource Constrained Devices
Cloud Authentication Server (CAS)
Resourceful User Devices
Login (EID, pwd)
SendOTP
EnterOTP
Authentication Verification
Authentication Acknowledgement
ReadData (CID)
Confidentiality Verification
SendData(CID,E[Data],T)
Mail_id Change (EID, pwd)
SendOTP
EnterOTP
Authentication Verification
Authentication Acknowledgement
Newmail_id
Mail id update Confirmation
Mble_noChange (EID, pwd)
EnterOTP
SendOTP
Authentication Verification
Authentication Acknowledgement
Newmble_no
Mble_no update Confirmation

Fig.7. Sequence of Operations of the ANNA Framework

Table.6. Details of the Data Collected

Data Collected	Details of the Data
CID	Patient Aadhaar Number
Name	Name of the Patient
Age	Age of the Patient
Sex	Sex of the Patient
Date	Date of the Medical Data Collected (DD-MM-YY)
Time	Time of the Medical Data Collected (Hr-mm-ss)
BP	Blood Pressure of the Patient at a particular time (mmHg)
SpO_2	Blood Oxygen of the Patient at a particular time (%)
HR	Heart Rate of the Patient at a particular time (bpm)

Table.7. Sample Medical Data

CID	Date (DD-MM-YY)	Time (Hr-mm-ss)	BP (mmHg)	spO_2 (%)	HR (bpm/min)
83001061	10-12-2017	10-11-31	120/80	99	84
15432451	10-12-2017	10-40-19	120/80	99	84
93147888	10-12-2017	10-27-52	140/90	98	70
83001061	10-12-2017	17-07-29	130/70	99	80
15432451	10-12-2017	17-28-47	130/70	99	84
93147888	10-12-2017	18-14-23	130/80	97	80
83001061	11-12-2017	10-10-50	130/70	99	80
15432451	11-12-2017	10-49-27	130/70	99	80
93147888	11-12-2017	11-20-31	120/90	99	82
83001061	11-12-2017	10-57-29	120/70	98	80

The security analysis of the proposed ANNA framework is experimented using Python Script and Wireshark simulator. Though Denial of Service (DoS), eavesdropping and Man-in-the-Middle (MitM) attacks are considered as the major security issues in Bluetooth, Wi-Fi and LTE Communications Technologies in healthcare IoT scenario respectively [18], the proposed block ciphers are resilience against these attacks. Moreover, due to the low memory capabilities and the limited computation resources [19], the majority of devices in IoT are vulnerable to resource enervation attacks. It is well suited for an insecure IoT enabled healthcare system in which sensitive information may be eavesdropped by a malicious user [21]. Practical experiment is conducted four times with the number of attacks 25, 50, 75 and 100. Finally, the results of the proposed block ciphers are compared and presented below. Man-in-the-middle attack: It is another type of eavesdropping attack. Here, the attacker communicates with the user independently and relays messages between them. But, the users believe that they are talking directly to each other over a private connection whereas the entire conversation is controlled by the attacker. In the proposed algorithm, the secret code is communicated directly to the user's registered mobile number and active for a minimum time interval.

If the time duration exceeds, it becomes inactive. So, the man-in-the-middle attack cannot succeed. A Comparison of Success and Failure Rates of MitM attack among the three proposed algorithms are presented in Fig.8 and Fig.9 respectively.

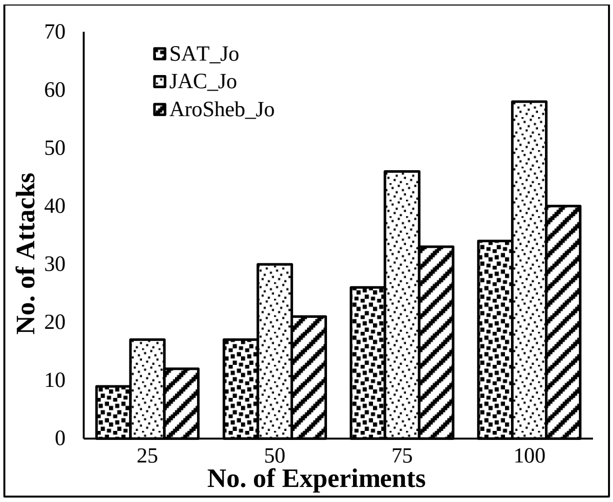

Fig.8. Comparison of Success Rate of MitM attack among the proposed algorithms

From the results presented in Fig.8 and Fig.9, it is proved clearly that the proposed algorithms are resilience against MitM attack. Denial of Service Attack: The implementation of IoT is hammered a lot by the Denial of Service (DoS) attack because of its resource limited nature. Different types of DoS attacks such as Jamming, Flooding, Tampering, etc. may spoil the nature of the IoT system. In the proposed framework, DoS attack is not possible because the encrypted data is exchanged only after the successful authentication. A Comparison of Success and Failure Rates of DoS attack among the proposed algorithms are presented in Fig.10 and Fig.11 respectively.

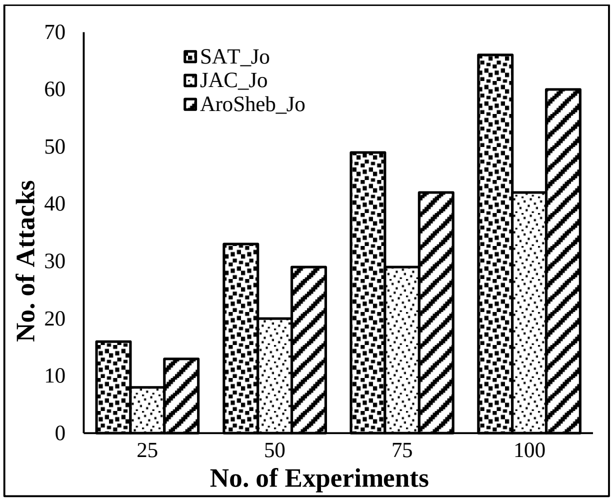

Fig.9. Comparison of Failure Rate of MitM attack among the proposed algorithms

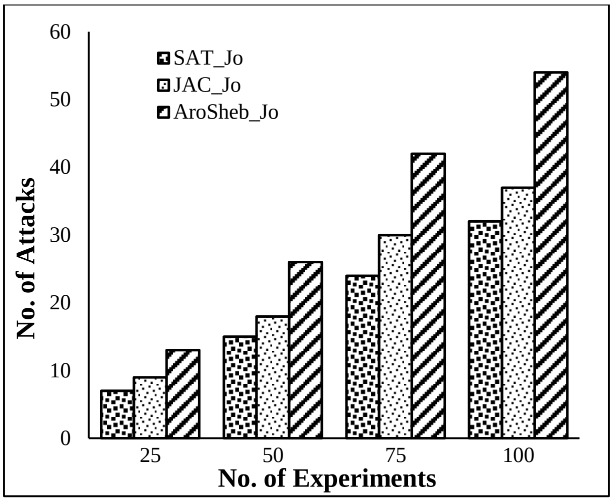

Fig.10. Comparison of Success Rate of DoS attack among the proposed algorithms

From the results presented in Fig.10 and Fig.11, it is proved clearly that the proposed algorithms present high level of security to the IoT healthcare data against DoS attack. Eavesdropping: It is nothing but secretly listening to a conversation/communication between two endpoints without any authorization. Here, in the ANNA framework, the computed *PID*, *DID* and *CID* are not communicated to the sender of the request. While any medical device tries to communicate with the *AS*, the *AS* immediately computes the *DID* from the *EPC* sent and verifies it with the *MD_Reg_Tab*. If match found, session key *SK* is sent to the *MD* along with the Time Stamp T_1. Otherwise, communication between the respective devices with the *AS* is not allowed. So, the possibilities of eavesdropping is restricted or avoided. A Comparison of Success and Failure Rates of Eavesdropping among the proposed algorithms are presented in Fig.12 and Fig.13.

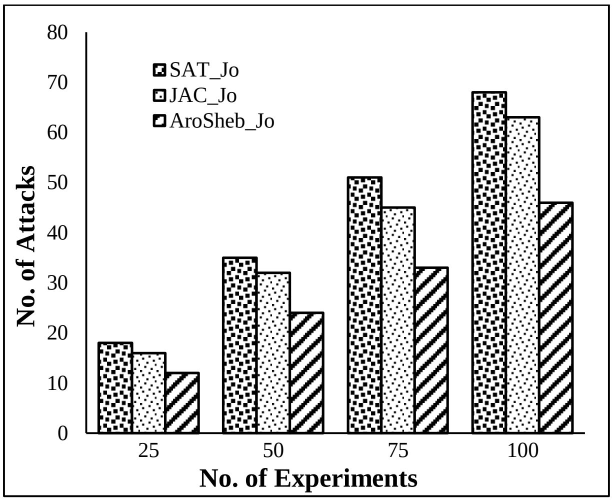

Fig.11. Comparison of Failure Rate of DoS attack among the proposed algorithms

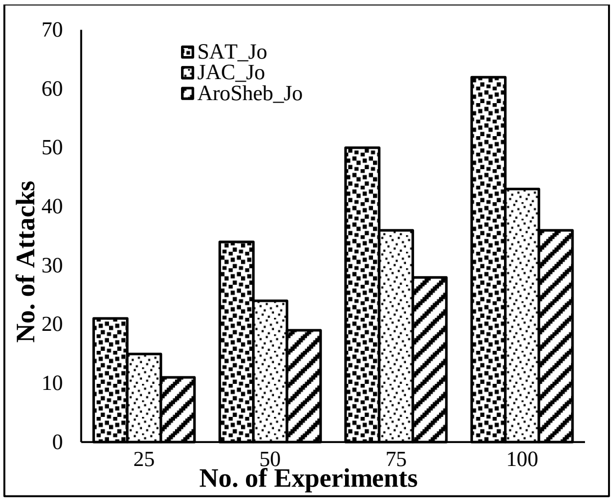

Fig.12. Comparison of Success Rate of Eavesdropping among the proposed algorithms

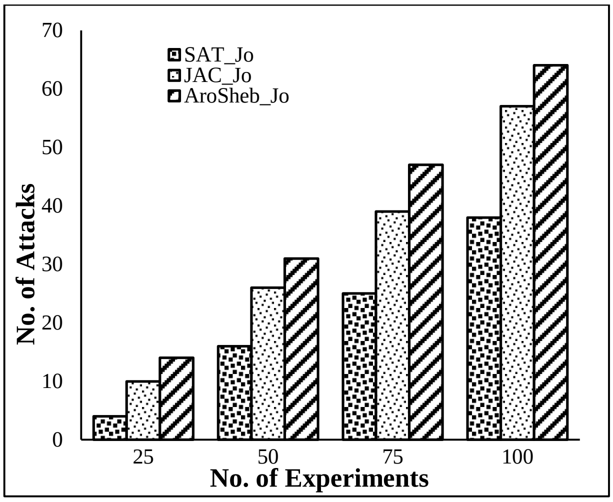

Fig.13. Comparison of Failure Rate of Eavesdropping among the proposed algorithms

From the results presented in Fig.12 and Fig.13, it is proved clearly that the proposed algorithms are resilience against Eavesdropping.

7. SALIENT FEATURES OF THE ANNA FRAMEWORK

The proposed ANNA framework aims at enhancing the security of data in the IoT enabled Smart healthcare system. It uses three lightweight algorithms namely *SAT_Jo*, *JAC_Jo* and *AroSheb_Jo* for secure accumulation and application of data of the ANNA framework. The salient features of this ANNA framework are listed below.

- Secure registration of stakeholders of the smart healthcare system.
- Secrete code for all the participants of the system.
- Lightweight security algorithm for secured transaction of medical data.
- Lightweight block cipher for securing the user credentials from malicious intruders.
- Secured data transfer to the user of the framework by unique and secure One Time Password.

8. CONCLUSION

Today is the era of Internet of medical devices which makes the hospital management smart and autonomous. Many researchers have been rigorously working to find different technological solutions to enhance medical services by mobilizing the potential of IoT. As part of this mission, this paper proposed a unified framework, ANNA, for enhancing the security of the healthcare IoT system by proposing three lightweight algorithms. In addition, this paper elaborated the working scenario of the ANNA framework with its methodological diagram. This framework could be implemented in primary health centres and remote village hospitals by which it could be beneficial to the rural and illiterate population of India.

REFERENCES

[1] Luca Catarinucci et al., “An IoT-Aware Architecture for Smart Healthcare Systems”, *IEEE Internet of Things Journal*, Vol. 2, No. 6, pp. 515-526, 2015.

[2] Uttam Kumar, “Evolution of IoT playing a crucial role in the healthcare sector”, Available at: http://www.dqindia.com/evolution-of-iot-playing-a-crucial-role-in-the-healthcare-sector/.

[3] S. Islam et al., “The Internet of Things for Health Care: A Comprehensive Survey”, *IEEE Access*, Vol. 3, pp. 678-708, 2015.

[4] David Niewolny, “How the Internet of Things Is Revolutionizing Healthcare”, Available at: https://www.nxp.com/docs/en/white-paper/IOTREVHEALCARWP.pdf.

[5] Aamir Hussain et al., “Health and Emergency-Care Platform for the Elderly and Disabled People in the Smart City”, *Journal of Systems and Software*, Vol. 110, pp. 253-263, 2015.

[6] Sarfraz Fayaz Khan, “Health Care Monitoring System in Internet of Things (loT) by Using RFID”, *Proceedings of 6th International Conference on Industrial Technology and Management*, pp. 198-204, 2017.

[7] Vikas Vippalapalli and Snigdha Ananthula, “Internet of Things (IoT) Based Smart Health Care System”, *Proceedings of International conference on Signal Processing, Communication, Power and Embedded System*, pp. 1229-1233, 2016.

[8] Prosanta Gope and Tzonelih Hwang, “BSN-Care: A Secure IoT-Based Modern Healthcare System using Body Sensor Network”, *IEEE Sensors Journal*, Vol. 16, No. 5, pp. 1368-1376, 2016.

[9] K. Natarajan, B. Prasath and P. Kokila, “Smart Health Care System Using Internet of Things”, *Journal of Network Communications and Emerging Technologies*, Vol. 6, No. 3, pp. 37-42, 2016.

[10] E. Kritika et al., “Multivariate Authentication and Encryption Scheme for Data Privacy in IoT Healthcare

Monitoring", *Imperial Journal of Interdisciplinary Research*, Vol. 2, No. 8, pp. 543-550, 2016.

[11] Byung Mun Lee, "Registration Protocol for Health IoT Platform to Share the Use of Medical Devices", *International Journal of Bio-Science and Bio-Technology*, Vol. 7, No. 4, pp. 1-10, 2015.

[12] Patrick Lacharme and Christophe Rosenberger, "Synchronous One Time Biometrics with Pattern Based Authentication", *Proceedings of International Conference on Availability, Reliability and Security*, 2016, pp. 1-7, 2016.

[13] Muthuraman Thangaraj, Pichaiah Punitha Ponmalar and Subramanian Anuradha, "Internet of Things (IOT) Enabled Smart Autonomous Hospital Management System-A Real World HealthCare Usecase with the Technology Drivers", *Proceedings of International Conference on Computational Intelligence and Computing Research*, pp. 1-8, 2015.

[14] R. Shantha Mary Joshitta and L. Arockiam, "SAT Jo: An Enhanced Lightweight Block Cipher for the Internet of Things", *Proceedings of IEEE International Conference on Intelligent Computing and Control Systems*, pp. 23-29, 2018.

[15] R. Shantha Mary Joshitta and L. Arockiam, "Device Authentication Mechanism for IoT Enabled Healthcare System", *Proceedings of IEEE International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies*, pp. 1-7, 2017.

[16] R. Shantha Mary Joshitta and L. Arockiam, "Key Generation Algorithm using Soft Set for Data Security in Internet of Things", *Proceedings of 3rd International Conference on Internet of Things*, pp. 367-372, 2018.

[17] R. Shantha Mary Joshitta and L. Arockiam, "Hybrid One Time Password Mechanism for User Authentication in Internet of Things Environment", *Journal of Advanced Research in Dynamical and Control Systems*, Vol. 3, No. 17, pp. 1547-1558, 2017.

[18] Wassnaa AL-Mawee, "Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey", Master's Thesis, Department of Computer Science, Western Michigan University, pp. 1-57, 2012.

[19] S. Santiago and L. Arockiam, "Energy Efficiency in Internet of Things: An Overview", *International Journal of Recent Trends in Engineering and Research*, Vol. 2, No. 6, pp. 475-484, 2016.

[20] R. Shantha Mary Joshitta and L. Arockiam, "Security in IoT Environment: A Survey", *International Journal of Information Technology and Mechanical Engineering*, Vol. 2, No. 7, pp. 1-8, 2016.

[21] L. Arockiam and S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, No. 8, pp. 3064-3070, 2013.