Mansoura Journal of Computers and Information Sciences

Enhanced Security of the Internet of Medical Things (IOMT)

I.S.Farahat

Department of Computer Science, faculty of computers and information, south Valley University, Luxor branch, Egypt

Hema_shwky@yahoo.com

A.S.Tolba

Department of Computer Science, faculty of computers and information, Mansoura University, Egypt

ast@astolba.com

Waleed Eladrosy

Department of Computer Science, faculty of computers and information, Mansoura University, Egypt

waleed_cs2000@yahoo.com

ABSTRACT

Healthcare is the major problem that faces the individuals around the world especially oldsters and disables. The development of the object to object technology (Internet of things (IoT)) is improved until it can be used to overcome the healthcare problem. The progress of the IoT extends to help the science in remote healthcare and predict the disease of the patients before it happened. But with these improvements the patient data become in danger because the patient data are sent from patient side over the internet to the physician so it becomes available for any attackers to attack the data and modified or stolen it in its way to the doctor or to the patient. So the healthcare field is having a security and privacy issue. This paper introduces system that can solve this problem by changing the data before it leaves the patient. So the transfer data is secured enough to protect the patients' data. The proposed system using a three technique one for encoding data to change the shape of data and compressed it and one technique for encrypt encoded data with AES but with rotated key and last one for make an authentication mechanism to protect data from output access and permit any person that have username and password credential to access patient's data. The authentication mechanism is built at the website with a private IP the proposed system is developed with low cost hardware to minimize the cost of the product with high efficiency.

Keywords

Internet *of medical things (IoMT),* threats *and attacks, security, encoding, decoding, encryption, decryption and authentication.*

1. INTRODUCTION

In 21st, the science especially computer science and information technology have moved towards to a new technology called internet of things (IoT). IoT field connects all objects surrounding us with each other by using some computing terms as the sensor, microcontrollers, transmitter, receiver and etc. [1]. IoT has a lot of application such as smart home, smart cities, agriculture in IoT and healthcare system. The available healthcare system is unacceptable because of the higher operational cost and not familiar with the patient [2]. So IoT move towards improving individual healthy. IoT in the field of a healthcare system is still in the first step of advancement [3] and it called internet of medical things (IoMT). IoMT is maintained by connecting some of the medical sensors with microcontrollers. Now, IoMT tries to connect all stakeholders of healthcare systems such as physicians, patients, and hospital staff although of their different locations. On the internet of medical things (IoMT) data move over the network to be sent from patient to physician to become easy for the physician to monitor his patient but hackers can attack this data over the network then modified this data it or steal it so the data have been transmitted over network become in a risk So the big challenge faces IoMT application is how to keep data secure.

One of the motivations behind the paper that Scientists agree that there are 6 technologies to make IoT network secure. The 6 technology are IoT Network Security, authentication, Encryption, security-side-channel attacks, Interface protection, Delivery mechanisms, System development and Security analytics and threat prediction [4] and also there is a report presented by Hewlett Packard on the state of security in the Internet of Things and internet of medical things and shows the risks that needed to get solution to protect and private the data of IoT. The following table (table 1) shows security problem that faces IoMT and IoT according Hewlett Packard report [5].

Table 1 security problems

Security problem	Percentage
Insufficient authentication	80%
Unencrypted communication	70%
Privacy concerns	80 %

The objective of our research is secure patient data, improve the health of the individual, and improve care quality, predict the disease before it happens and maintain patient data privacy. This paper focuses on creating an IoMT security system with the advantage that system is robust, low cost hardware and free software source. The task of the proposed system is secure and private all human vital parameter that is measured by the medical sensor and transfers the secured data to the physician over the internet So the main concern of is reset of this paper is make an authentication, encryption and encoded method to secure this data. In section II, the paper introduces the internet of things and its application and introduce internet of medical things than discuss the challenge face IoMT. In Section III, paper discuss some of the related work, and the paper describes the proposed system in section IV, then the paper presents the result and performance evaluation at section V, at section VI, the paper concludes the work and introduce our future works.

2. Background

Internet of things is the five stage of the development of the internet [2]. The following figure (fig1) shows the stage of the development internet.

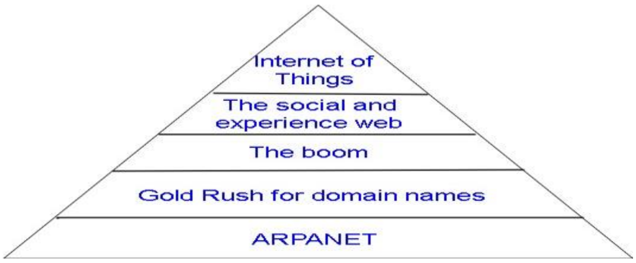

Fig 1 five stage of the development of the internet

Internet of things is the thing to thing communication that depends on the small thing called sensor which is responsible for gather data from the environment and sent the data to microcontrollers [6]. In IoT, sensors collect data of environment to be used anywhere and anytime and processing this data in any way [7]. IoT is not a new technology since there are 18.2 billion devices are connected through IoT concept so it is a hot field in the world nowadays [8]. Internet of things has a lot of application so the paper discusses the application of IoT at first.

A. *Application of IOT*

From building automation and smart factories to wearables, the IoT is omnipresent on every side of our lives. It makes developing applications simpler with hardware, software, and assistance to link anything to the internet. IoT pledge to bring formidable value to the life of the people. If we are able to connect all things in our world, we will achieve labor that will really seem like the charm. But because IoT is the vast field and far-reaching of a concept, we have found that many are confused about what the potential applications for IoT are exactly. But because IoT is the vast field and far-reaching of a concept, we have found that many are confused about what the potential applications for IoT are exactly. Table 2 gives some Internet of Things applications to clear thing up. In the following table, we will identify six key markets for the IoT with potential for exponential growth.

Table 2 application of IoT

IoT application	Descriptions
Smart Home	The smart home is probably the most communal IoT application at the moment because it is the one that is most affordable and easily available to consumers. There are hundreds of products on the market that users can control with their voices to make their lives more connected than ever [9].
Wearables	Watches are no longer just for showing time. The Apple Watch and other smart watches on the market have changed our wrists into smartphone holsters by allowing text messaging, phone calls, and more. And devices such as Fitbit and Jawbone have revolutionized the fitness world by supplying people more data about their workouts [10].
Smart Cities	The IoT has the Ability to mutate entire cities by resolving real problems citizens face each day. With the suitable connections and data, the Internet of Things can resolve traffic congestion problems and decrease noise, crime, and pollution [11].
Connected Cars	These vehicles are linked with Internet access and can share that access with others, just like connecting to a wireless network in a home or office. More vehicles are beginning to link with this functionality, so be prepared to see more apps included in future cars[12].
IoT in Agriculture	With the continuous rise in world's population, request for food supply is extremely raised. Governments are helping farmers to use advanced techniques and research to raise food production. Smart farming is one of the fastest growing fields in IoT [13].
Healthcare	Healthcare Connected healthcare yet remains the sleeping titan of the Internet of Things applications. The connotation of the connected healthcare system and smart medical devices endure massive potential not just for companies, but also for the well-being of people in general. Research proves that Internet of Things in healthcare will be enormous in next years. IoT in healthcare is looking forward to enabling people to live healthier lives by wearing connected devices. The collected data will help in the personalized analysis of an individual’s health and provide tailor-made strategies to combat illness [14].

The advancement of the IoT leads a big revolution in the Healthcare the big example that describes the pervious statement that 60 % of the organization has already changed their traditional healthcare system to IoMT systems because they realize that IoMT saves costs, improve their visibility, customer experience and incoming money [16]. Because of increasing the reliability, accuracy and good work of the microelectronics and sensor devices, IoT plays an important role in the healthcare field. Researchers are the concern with a connecting medical sensor and introduce healthcare services to make a digitalize IoMT product that helps individuals [17]. According to WHO, Pakistan faces a problem of health and the average age of people in Pakistan are 64.5 years for males and 67.3 years for females [15] So the existence of IoT field in the healthcare system is very important now to these countries. According to Reenita Das report at Forbes, there are ten Ways the Internet of Medical Things Is Revolutionizing Senior Care such as Vitals-Tracking Wearable, Medication Adherence Tools, Virtual Home Assistants, Portable Diagnostics Devices and Personal Emergency Response Systems [18].

This paper focuses on develops portable Diagnostics devices this help patient to save his health. IoMT system must be consisting of the two system one for patient and another for physician system and internet between them. The remote healthcare system is described in the following figure (fig 2).

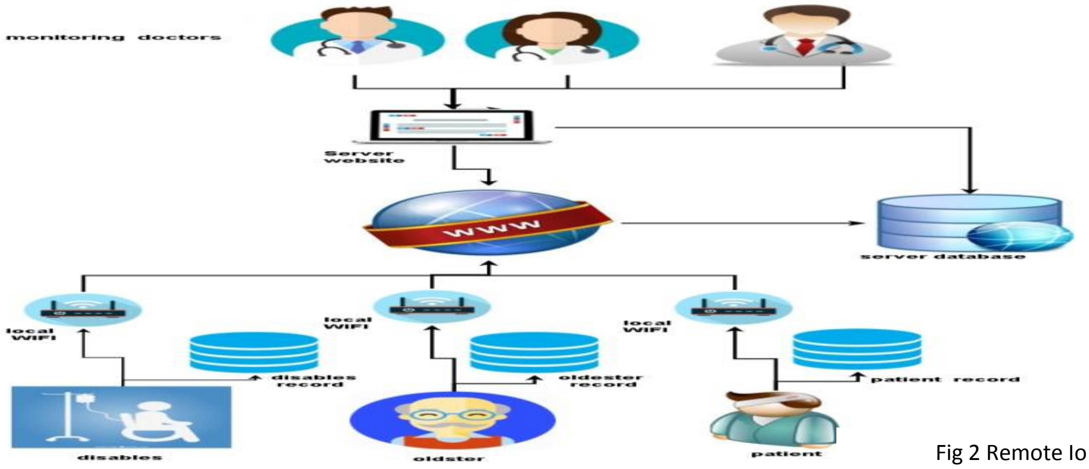

Fig 2 Remote IoMT Model

To take about IoMT it must be the first take about body area network (BAN) which is the network of some of the medical sensor that built in the human body and microcontrollers such as the following figure (fig 3).

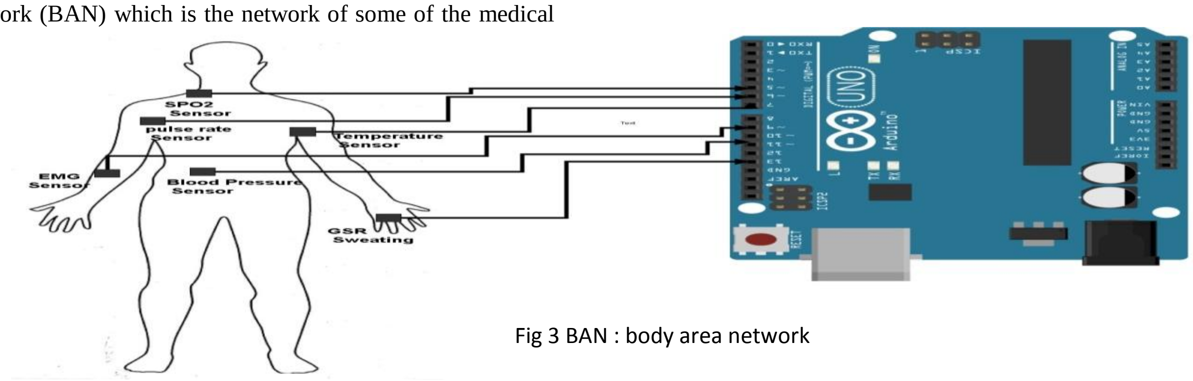

Fig 3 BAN : body area network

With the increase of the number of sensors, it will lead to complex circuits so IoMT system needs E-health shield that collects all sensors in one place and avoids the complex circuits. The following figure shows the sensor needed to make healthcare system and the shield needed (fig 4).

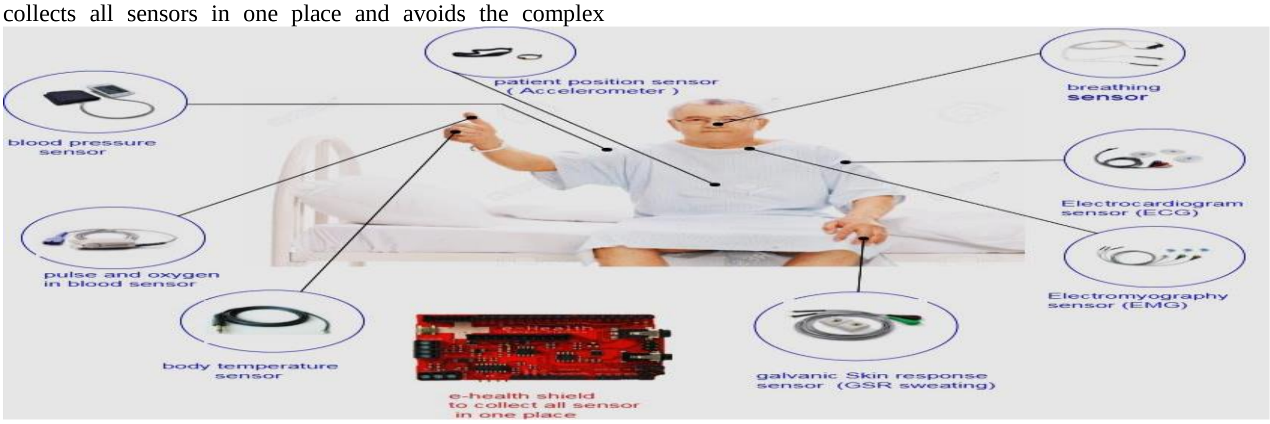
patient position sensor (Accelerometer)
breathing sensor
blood pressure sensor
Electrocardiogram sensor (ECG)
pulse and oxygen in blood sensor
Electromyography sensor (EMG)
body temperature sensor
e-health shield to collect all sensor in one place
galvanic Skin response sensor (GSR sweating)

Fig 4 Healthcare sensors and shield

By using the previous method the data of patient become available and easy to stolen or modified before sending patient data to doctor so Security and privacy of the patient's data is the main concern of the IoMT. Patients' record must be secure and private because it holds personal information and it private to patients. According to Gartner forecast, there are 8.4 billion internet-connected IoT devices in use currently and most new business systems and business processes will incorporate IoT[19].

Although the patients' records must be private and secure it must be available for all authorized people such as physician or nurses or hospitals staff at all time and thus can happen by making an authentication method to permit anyone to have credentials to access this data. To secure data we must achieve three points the following table (table 3) describe the three points to achieve security [20].

Table 3 security challenges

Property	Descriptions

Confidentiality	Confidentiality refers to anyone can access patients data must be the confident person to leave that information to access by him. When the communication between two parties in a relationship such as patient and doctor, this is meaning that this communication has Confidentiality property.
Privacy	Privacy is the distinct from confidentiality because privacy is the patient has a right to access the data alone without sharing that data with any person
Security	Security is mean how to protect the private patients" data from the access from output access and don't let anyone see it before show his credentials.

Any Security System must have an encryption method and authentication method to achieve the previous three point of security.

3. Related work

The security and privacy issue are the big challenge that faces IoT from the beginning of the appearance of the field[21].at first scientists think to build an architecture that divides the problem into parts and solves each part. One example of this architecture is open web application security project (OWASP). OWASP is an organization that focuses on increasing the security of any open source software. OWASP develops a medical device that helps healthcare to the secure patients' data [22]. CGI's white paper [23] starts to get a solution for improving the security and privacy of healthcare system. Some research started to interest in the security of healthcare system that pushes Lobna Yehia et al to describe some of the application that helps in secure data on the internet of medical things field[24]. Lastly, in 2017, Muhammad Usman et al develop a lightweight encryption technique that changes the shape of the data by the mix between two encryption method and this method is described in [25].

Scientist in all previous work try to developed software that solve security problem but there is scientist that try to solve the problem by building hardware that solve security problem. Feldhofer [26] start to think to make an encryption technique using hardware by make encryption using AES method in RFID but it cost a lot of gates and store the small number of bits [27]. Jung et al developed a method with using a minimum number of gates by comparing by Feldhofer [28]. This problem of a large number of gates push scientist to use a another method of encryption but using the hash function and this describes in [28][29][30] But the disadvantage of this method is needed to store two states of function so it's overload to the circuits. Peris et al think to use a lightweight algorithm for encryption and using an authentication method that results from a low cost and the little number of the gate[30] but with a limitation in an RFID. The scientist starts to think in another solution to secure data because the problem that faces them in using RFID so two methods appear with make an authenticated encryption algorithm but between the tag and the reader [31][32]. But all method of try to use hardware is failed because the attackers hack them before [33].so the researchers move towards encrypting data at communication level [34] but it will cause a lot of problem such as delay, lose in the packet and need a lot of energy and power[35] so researcher now using a lightweight encryption technique such as [36][37]. No one can develop a public key method because it needed a lot of processing which no Arduino kit can hold [34].

4. WIFI security system

The component of the proposed system is illustrated in the following table (table 4).

Table 4system hardware specification

COMPONENT TYPE	NAME
Kit	Esp2866wifi module
Sensors	Lm35 sensor
Breadboard	Breadboard
Electric Cable	Hook up wires

The following figure (fig5) shows server side in the proposed system.

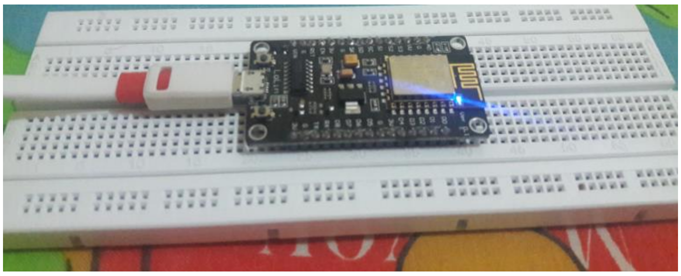

Fig 5 Server side of the proposed system

Figure 6 (fig 6) illustrates the client side in the proposed system

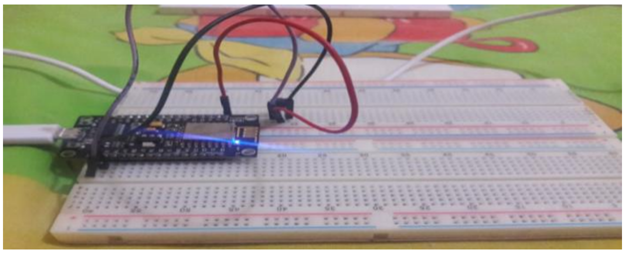

Fig 6 Client side of the proposed system

The following figure illustrates the block diagram that describes the proposed security system

.

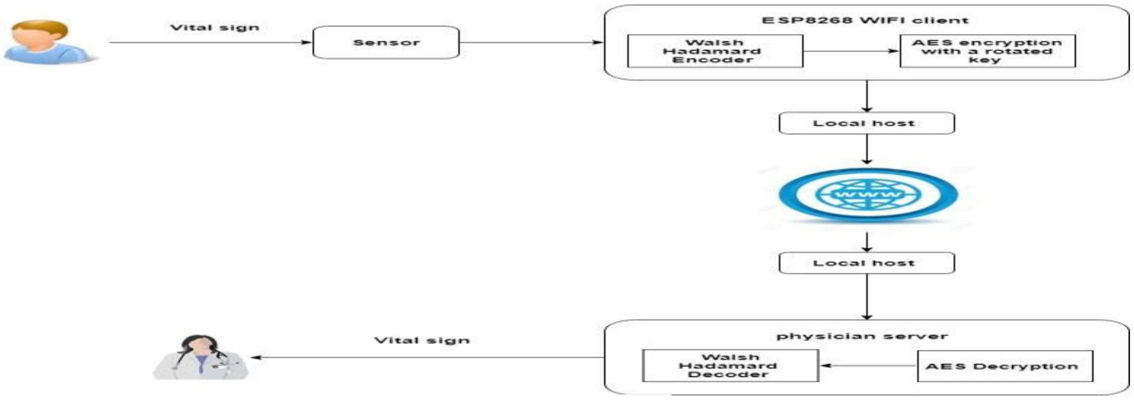

Fig 7 Security system block diagram

The security proposed system is divided into two system, the first system is in patient side which is consist of two algorithms one for encryption and other one for encoding. The second system is in physician side which decrypt and decoding the data to get the original data. The proposed system encrypts data and decrypts it by using key with 256 bit length and block size with 128 bit length.

The following table describes each notation that used in the algorithm (table 5) [38].

Table 5 notation table

Notations	Meaning
$\mathbf{D}_i$	**Physician i**
$\mathbf{P}_i$	**Patient i**
$\mathbf{C}_i$	**Client side**
$\mathbf{S}_i$	**Physician server**
$\mathbf{R}_i$	**Rotated key i**
$\mathbf{V}_i$	**Patient vital signs of $\mathbf{P}_i$**
$\mathbf{T}_i$	**Temperature $\mathbf{T}_i$**
$\mathbf{SE}_i$	**Sensor**
$\mathbf{OD}_i$	**Original data**
$\mathbf{AD}_i$	**ASCII of $\mathbf{OD}_i$**
$\mathbf{MD}_i$	**ASCII data $\mathbf{AD}_i$ but in the shape of matrix**
$\mathbf{MeD}_i$	**Encoded matrix data**
$\mathbf{E}_i$	**Encoded data**
N	**Shift magnitude of $\mathbf{k}_i$**
k_i	Key of encryption
$\mathbf{ST}_{i,j}$	**State of data (data in two dimension array form)**
$\mathbf{R}_{i,j}$	**Round key**
SD	**SubBytes process**
$\mathbf{SR}_{i,j}$	**Data after shift row process**
L	**Shift magnitude of shift row process**
R	**Number if rows**
$\mathbf{CM}_{i,j}$	**Is a fixed matrix $\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$ to make mix column process**
$\mathbf{EE}_{i,j}$	**Encoded encryption data in a form of two dimension array**
$\mathbf{EED}_i$	**Encoded encryption data**
$\mathbf{k}_{n-i}$	**Last key use in encryption**
$\mathrm{CM}_{i,j}^{-1}$	Is a inversed matrix of $\mathrm{CM}_{i,j}$ $\begin{bmatrix} E & B & D & 9 \\ 9 & E & B & D \\ D & 9 & E & B \\ B & D & 9 & E \end{bmatrix}$
$\mathbf{MC}_{i,j}$	**Data after mix column process**
$\mathbf{V}_i$	**Value of encoded data $\mathbf{E}_i$**
$\mathbf{RE}_i$	**Length of encoded data**
$\mathbf{AED}_i$	**Message$\mathbf{E}_i$ from ASCII**
$\mathbf{ID}_i$	**Username of $\mathbf{D}_i$stored in code**
$\mathbf{PW}_i$	**Password of $\mathbf{D}_i$ stored in code**
H	**Validity check**
$\mathbf{U}_i$	**Username that $\mathbf{D}_i$ entered**
$\mathbf{PASS}_i$	**Password that $\mathbf{D}_i$ entered**

The idea is helping physician D_i to monitor the status of his patients P_i, so the patient's data V_i need to send to server side S_i through the internet but the data become may be stolen or modified so before sending the patient's data to physician, the Data must be encrypted at client side C_i . The proposed system is encoded data with Walsh Hadamard and then encrypts data by encrypting it with AES method with using the rotated keyR_i then C_i send this data to local wifi then local wifi send receives encoded and encrypted data $EED_i$to server side S_i,S_i start to decrypt EED_i using same K_i which is rotated every round then decoded it to facilitate the ability of physician D_i to access the patients P_i data. To protect the patients' P_i data from outside access an authentication method is applied to system to overcome this problem so the proposed system is divide into two main algorithm on for describe encryption and encoding technique and called Sensor Data authenticated encoding and Encryption Algorithm and the other one is for describe decoding, decryption and authentication technique and called Sensor Data authenticated decoding and Decryption Algorithm.

A. Sensor Data authenticated encoding and Encryption Algorithm

The following steps present our sensor data authenticated encoding encryption algorithm:

Algorithm 1 encoding encryption algorithm

1. *Patient vital signs V_i has been measured by sensors such as temperature*
2. *Data $OD_i$is encoded by The ESP8266 of client side $C_i$by using Walsh Hadamard*
3. *Encoded data E_i is encrypted by using by a synchronizer key k_i to apply AES method but with rotatedk_i.*
4. *Encrypted data $EED_i$is sent to local Wi-Fi through ESP2866 of client side C_i*
5. *Encrypted data $EED_i$is sent to ESP6288 of physician server S_i through Local Wi-Fi*

Authenticated encoding and Encryption Algorithm can be comprised into 3 phases acquiring phase, encoding phase and encryption phase.

Acquiring phase

In this phase sensor $\mathrm{SE_i}$ detect data and send it to client side $\mathrm{C_i}$. The following table (table 6) shows the steps that the proposed system takes to acquiring data.

Table 6 acquiring phase

Step name	Description
(A1)	Sensors SE_i detect patient vital signs V_i such as e.g. temperature T_i
(A2)	Sensors SE_i send this data OD_i to client sideC_i.
(A3)	$\mathrm{C}_i$receivedOD_i.

Encoding phase

In this phase data $\mathrm{od_i}$ can be encoding with fast Walsh Hadamard encoding method. The following table (table 7) shows the steps that the proposed system takes to encoding data with Walsh Hadamard.

Table 7 encoding phase

Step name	Description
(E1)	C_i Convert OD_i to the equivalent ASCII code AD_i.
(E2)	C_i Insert AD_i in a matrix MD_i where each ASCII of data is represent an element in a matrix MD_i but matrix MD_i should to be with a length of 2 or power of 2.
(E3)	$\mathrm{C}_i$start to encode the MD_i by add each element of MD_i to MD_{n-i} until n/2 where n is size of matrix and start add from first element with index 0 to index n/2 element and subtract each element of MD_i to MD_{n-i} from first element with index n/2 +1 to element with last index and store this new matrix in MeD_i
(E4)	Divide the matrix MeD_i to two matrixes and then do step E3 to each matrix.
(E5)	C_i Repeat step from E3 to E4 until when divide matrix to one element in each matrix
(E6)	Subtract each element from 256 to ensure that each element is from the range 0 to 255 but apply subtract the element from 0 to N/2 index number
(E6)	Get the ASCII MeD_i and store it in matrix E_i

Encryption phase

In this phase encoded data$\mathrm{E_i}$ can be encrypted with AES method but with a rotated key$\mathrm{k_i}$. The following table (table 8) shows the steps that the proposed system takes to encrypt data with AES with rotated key.

Table 8 encryption phase

Step name	Description
(EE1)	$\mathrm{C}_i$compute new key $\mathrm{k}_i = \mathrm{k}_{i-n}$ then C_i repeat this step if i>length(k_i)
(EE2)	$\mathrm{C}_i$compute$\mathrm{ST}_{i,j}$=E_i
(EE3)	$\mathrm{C}_i$computes$\mathrm{R}_{i,j}$ =$\mathrm{ST}_{i.j} \oplus \mathrm{k}_i$ then C_i compute $\mathrm{SB}_{i,j}$=SD($\mathrm{R}_{i.j}$)
(EE4)	C_i computes $\mathrm{SR}_{i.j} = \mathrm{SB}_{i,j-L}$ while L=0 at first then repeat with increase L by this equation L=L+1 if l<R and this called s-byte or s-box
(EE5)	$\mathrm{C_i}$computes$\mathrm{EE_{i,j}} = \mathrm{SR_{i.j}} \otimes \mathrm{CM_{i,j}}$ then$\mathrm{C_i}$ compute $\mathrm{ST}_{i.j} = \mathrm{EE_{i,j}}$
(EE6)	$\mathrm{C_i}$computes a key expansion $\mathrm{k_i}$:$\mathrm{w_0}$=$\mathrm{k_{i-1}}$: $\mathrm{w_0} \oplus$ SD($\mathrm{k_{i-1}}$: $\mathrm{w_3} \gg 8 \oplus$ $\mathrm{recon_i}$) then compute $\mathrm{k_0}$=$\mathrm{w_i}$:$\mathrm{k_{i-1}}$: $\mathrm{w_i} \oplus$ SD($\mathrm{k_i}$: $\mathrm{w_{i-1}}$) then $\mathrm{C_i}$ repeat steps from (EE3) to (EE6) until a number of round determined but if I is a last round escape step (EE5)
(EE7)	$\mathrm{C}_i$computes$\mathrm{E}ED_i = \mathrm{E}E_{i,j}$ then C_i send $\mathrm{E}ED_i$ to local WiFi

After encryption phase local wifi send data to server side $\mathrm{S_i}$where data can decrypted and decoded.

B. SENSOR DATA AUTHENTICATED DECODING AND DECRYPTION ALGORITHM

In this section data decryption, decoding and authentication will be discussed. The following steps are our sensor data authentication decryption algorithm:

Algorithm 2 decoding decryption algorithm

1. *Physician side S_i using the rotated key $K_i$to decrypt EED_i that sent from patient side*
2. *Physician side S_i decode E_i to get the original data OD_iusing the reverse Walsh Hadamard*
3. *Physician side S_i is upload data to website build upon S_i with an authentication method.*
4. *The doctor D_i can open a website with his credentials then access patients' data.*

Authenticated decoding and Decryption Algorithm can be comprised into three phases decryption phase, decoding phase and authentication phase.

Decryption phase

In this phase server side S_i decrypts encryption encrypted data EED_i WITH AES method with a rotated key k_i . The following table (table 9) shows the steps that the proposed system takes to decrypt data.

Table 9 decryption phase

STEP NAME	DESCRIPTION
(D1)	**LOCAL WIFI SEND EED_i TOS_i**
(D2)	**S_iCOMPUTES NEW KEY $k_i = k_{i-n}$ THEN S_i REPEAT THIS STEP IF I>LENGTH(k_i)**
(D3)	**S_iCOMPUTES$ST_{i,j}$=EED_i**
(D4)	S_i computes $R_{i,j}$ =$ST_{i.j} \oplus k_n$ then $S_i$compute $SR_{i.j} = R_{i,j+L}$ while L=0 at first then repeat with increase L by this equation L=L+1 if l<R
(D5)	**S_iCOMPUTE$SB_{i,j}$=SD($SR_{i.j}$)**
(D6)	S_i computes $R_{i,j}$ =$SB_{i,j} \oplus k_{n-i}$ then S_i computes $MC_{i,j} = R_{i.j} \otimes CM_{i,j}^{-1}$
(D7)	S_i compute $SR_{i.j} = MC_{i,j+L}$ while L=0 at first then repeat with increase L by this equation L=L+1 if l<R
(D8)	S_i compute $EE_{i,j}$=SD($SR_{i,j}$) then S_i compute $ST_{i,j} = EE_{i,j}$
(D9)	C_i computes a key expansion k_{n-i}:w_0=k_{n-i+1}: $w_n \oplus$ SD(k_{n-i+1}: $w_{n-3} \ll 8 \oplus recon_i$) then compute k_n=w_{n-i}:k_{n-i+1}: $w_{n-i} \oplus$ SD(k_{n-i}: w_{n-i+1}) then s_i repeat steps from (E5) to (D7) until a number of n-i<0
(D10)	**S_iCOMPUTES$E_i = EE_{i,j}$**

Decoding phase

In this phase server side S_i Decode encoded data E_i With Walsh Hadamard method. The following table (table 10) shows the steps that the proposed system takes to decoding data.

Table 10 decoding phase

Step name	Description
(DD1)	S_i Convert E_i from the ASCII code to AED_i.
(DD2)	Add eaxh element to 256 to return the message MED_i but apply subtract the element from 0 to N/2 index number
(DD3)	S_i compute MD_i by make reverse of Fast Walsh Hadamard by start with two following element in and then use 4 element to get original message and store it in MD_i
(DD4)	S_i Convert MD_i from ASCII code and store it in OD_i.
(DD5)	S_i Upload OD_j to website that is created inS_i

Authentication phase

In this phase doctor d_i require authentication to monitor patient through a website that located in a server side. The following table (table 11) shows the steps that the proposed system takes to prove that data is authenticated.

Table 11 authentication phase

Step name	Description
(AU1)	D_i Enter name of website or ip of website eg. 192.168.1.80.
(AU2)	Website need authentication by ID_i and PW_i
(AU3)	$D_i$enterU_i and $PASS_i$ in the website authentication form then S_i compute $H=U_i \oplus ID_i \&\& PASS_i \oplus PW_i$
(AU4)	IF H=0 then $S_i$permit D_i to monitor p_i if H≠0 repeat from step (AU2)

5. Experimental Results and Discussion

The proposed system contains two components ESP2866 kit with the lm35 sensor at the client side and ESP2866 kit at the server side. The results of encryption and encoding on the client side and results of decoding and decryption at the server side will be presented in this section.

A. Results at client side

At the first sensors acquire data from patient and send it to ESP2866 kit for example a temperature sensor lm35 measures the temperature of patient and sent it to patient kit at which it converts to its ASCII code and then decoded with Walsh Hadadmard then subtract each element from 256 to convert the message to its ASCII code again but apply subtract the element from 0 to N/2 index number then the result message from encoding is encrypted using AES method but with a rotated key to prevent any one to access this message in the way to doctor. The following table (Table 12) shows the measurements of the lm35 temperature sensor and the message after encoding, conversion to ASCII and encryption.

Table 12 results at Client side

Step	**Result**	
Data from sensors	**23.85**	**17.72**
Fast Walsh Hadamard encoded message	**288 10 84 30 118 -32 -86 -12**	**287 3 85 21 123 -33 -79 -15**
After subtract each element from 256	**33 -245 -171 -255 118 -32 -86 -12**	**32 -252 -170 -234 123 -33 79 -15**
ASCII of encoded message	**! U v□ □**	**V$_T${□□ V$_T${□□**
Message send to the server	**FT□ □4NTK □ □O**	**□w□ □ □!-□e□2k**

The following table (table 13) shows how the data encryption and decoding when enlarging data

Table 13 results at Client side when enlarge data

Step	**Result**	
Data from sensors	**20.10001**	**20.01122**
Fast Walsh Hadamard encoded message	**386 -2 2 6 0 0 4 4 386 -2 2 6 0 0 4 4**	**390 0 2 4 -6 0 6 4 390 0 2 4 -6 0 6 4**
After subtract each element from 256	**131 -257 -253 -249 -255 -255 -251 251 386 -2 2 6 0 0 4 4**	**135 -255 -253 -251 -261 -255 -249 -251 390 0 2 4 -6 0 6 4**
ASCII of Encoded message	□ □⌐||□ □¬-	□⌐|□|□
Message send to the server	**yT$□ □ □뜰□u□ □K□d**	**Ǽ□/□ □ □ □ □ □z/□+□}**

B. Result in server side

The server side receives the encrypted encoded message then the server starts to get the original message by decrypting data using ASE method but with rotated key and then add 255 to each element from the 0 to N/2 index number and then decoding it by doing reverse Walsh Hadamard.

The following table (table 14) shows how the receiver get original message.

Table 14 results from Server side

Step	**Result**	
Message received from the patient's client	**FT□ □4NTK □ □O**	**□w□ □ □!-□e□2k**
Decrypted Message	**! U v□ □**	**V$_T${□□ V$_T${□□**
Add256 to each element until element with n/2 index number	**33 -245 -171 -255 118 -32 -86 -12**	**32 -252 -170 -234 123 -33 79 -15**
ASCII Conversion and Fast Walsh Hadamard decoding	**288 10 84 30 118 -32 -86 -12**	**287 3 85 21 123 -33 -79 -15**
Message send to the server	**23.85**	**17.72**

The following table (table 15) shows the result when enlarging data:

Table 15 results from Server side when enlarge data

Step	**Result**	
Message received from the patient's client	**yT$□ □ □뜰□u□ □K□ d**	**Ǽ□/□ □ □ □ □ □z/□+□}**
Decrypted Message	□ □||□ □¬-	□⌐|□|□
Add256 to each element until element with n/2 index number	**131 -257 -253 -249 -255 -255 -251 251 386 -2 2 6 0 0 4 4**	**135 -255 -253 -251 -261 -255 -249 -251 390 0 2 4 -6 0 6 4**
ASCII Conversion and Fast Walsh Hadamard decoding	**386 -2 2 6 0 0 4 4 386 -2 2 6 0 0 4 4**	**390 0 2 4 -6 0 6 4 390 0 2 4 -6 0 6 4**
Message send to the server	**20.10001**	**20.01122**

Then the original data is uploaded to a website that is built at a server side but its authenticated website. If a doctor wants to show patient data he must enter his name and his password to access this data.

6. performance evaluation

There are two main things to compare between encryption algorithms with another is how the data is secure enough and the speed of the method used. The proposed system is working without the intervention of human and the key is coding is in hardware kit so it's difficult to attack and get the key from hardware because most of the attacks use malicious software to attack any person but there no intervention of the user to active this malicious software.

The proposed system consist of encoding and encryption so the data is changed more than one time so it difficult to predict or get this data by trying because it will cost a lot of time to get it. The following table (table 16) compares between the proposed system and another method in a time (microsecond) with small data.

Table 16 Evaluation Performance with small data

Algorithm`	**BytesProcessed**	**Encrypt and encode Time** (ms)	**Decrypt and decode Time** (ms)

AES with rotated key with Walsh Hadamard encoding	8	14440	11980
AES	8	14343	11908
DES	8	18435	18432
3DES	8	55657	54158

The table shows that our method takes less time than the other methods except for AES method because the proposed system uses AES and Walsh Hadamard. The difference time between AES and the proposed system is that the proposed system is acceptable while we change the shape of the data. The following table (table 17) compares between the proposed system and another method in a time (microsecond) when enlarging data.

Table 17EvaluationPerformance with large data

Algorithm	BytesProcessed	Encrypt and encode Time (ms)	decrypt and decode Time (ms)
AES with rotated key with Walsh Hadamard encoding	4,096	36323	35689
AES	4,096	30386	29941
DES	4,096	40105	38325
3DES	4,096	130947	129814

The table (table 17) show that the method using a compression technique so when large data it perform fast than another method except for AES method. The following figure (fig 8) shows the chart of each method by using the result of the previous two tables.

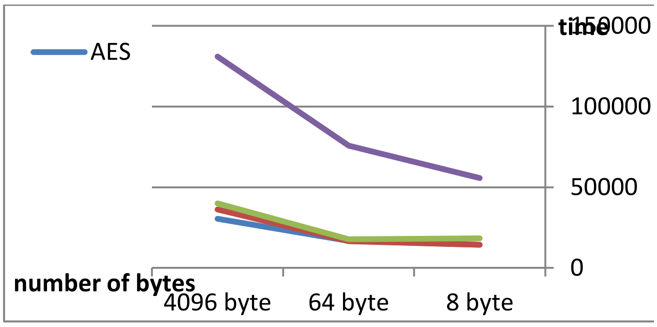

Fig 8 chart of the time difference of methods

The pervious result prove that AES method is better than the proposed system in a time but the following table (table 18) prove that the proposed system is more secure than AES.

Table 18 difference between AES and proposed system

Factor	AES method	Walsh Hadamard with AES
Key	Use same key	Key change after each encryption
Time	Less	More
Implementation place	Any place	Embedded in hardware
Iteration to hack	Less	More
Destination	Don't have authentication method	Have authentication method to get data

The previous table shows that the proposed system is secure by comparing with AES with the factors like the encryption key, in the proposed system is changed so if the attacker gets the data or key, he can't use it to get the next data but with comparing with the time AES is better than the proposed system because the proposed system use Walsh Hadamard with AES. The main factor that distinct the proposed system is it embedded in hardware without the intervention of individual so it difficult to hack because a lot of hack method depends on the human that active their malicious software but AES is software can implement in any computer so it can hack. The number of iterations needs to penetration the data is nine cycle but the proposed system use AES and also the data is changed many times by decoding it and convert it to ASCII so it needs much time to penetrate it. The proposed system is developed with an authentication method to permit any person to get data except that one has credentials to access data.

computational complexity of encoding and Encryption algorithm is O(n log n+mc+k) where k is key length, n is original data length, m is the number of round and c is a scaling factor depending on whether you're using 192 or 256-bit keys. Since m and c is constant so time complexity at client side is O (n log n +k). The computational complexity of decoding and decryption algorithm is O(n log n+mc+k) Since m and c are constant so time complexity at client side is O (n log n +k).

In The paper [36] show that SIT method take 3006 cycles and AES method take 2739 cycle when encrypted 64-bit data, if we suppose that each cycle takes 1ms and this is little by knowing that AES take 14343 ms when encrypted 8 data then the SIT takes 26739 ms and AES takes 3006ms. The difference between the time of two methods is 267 and when using a enlarge data this difference will be increased but the time difference in the proposed system when encrypting 64 data is increase by n log n while comparing with AES method so the difference is 115.59 microsecond, so the proposed system is good in a time than SIT method.

7. Conclusion

In this paper, the proposed system introduces an encryption encoding method to secure patient's data and presents an authentication method to prevent anyone to access this data except anyone who have a credentials (username and password).

Our future work is increasing the number of the sensor in our system, and we will focus on making the shield for collector IoMT sensors without using complex circuits and we will increase the flexibility of the proposed system by trying to encrypt binary data like the image. The main concern in the future work is testing the proposed system with protocols like TCP, UDP.

REFERENCES

[1] K. Karimi and G. Atkinson, "What the Internet of Things (IoT) needs to become a reality," *White Pap. Free. ARM*, pp. 1–16, 2013.

[2] S. R. Basavaraju, "HEALTH CARE DATA ANALYTICS FOR ADAPTABILITY IN E-HEALTH CARE NETWORKS," 2016.

[3] A. Kulkarni and S. Sathe, "Healthcare applications of the Internet of Things: A Review," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 5, pp. 6229–6232, 2014.

[4] http://www.electronicdesign.com/industrial-automation/8-critical-iot-security-technologies,August 2017 (last access 10 October 2017)

[5] http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.Wmb4t66WbIU, July 2014 (last access 15 November 2017)

[6] https://www.sas.com/en_us/insights/big-data/internet-of-things.html, 2017 (last access 5 September 2017)

[7] P. G. Benardos and G. C. Vosniakos, "Internet of things and industrial applications for precision machining," in *Solid State Phenomena*, 2017, vol. 261, pp. 440–447.

[8] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, November 2016 (last access 20 November 2017)

[9] B. L. R. Stojkoska and K. V Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *J. Clean. Prod.*, vol. 140, no. Part 3, pp. 1454–1464, 2017.

[10] W. Sun, J. Liu, and H. Zhang, "When Smart Wearables Meet Intelligent Vehicles: Challenges and Future Directions," *IEEE Wirel. Commun.*, vol. 24, no. 3, pp. 58–65, 2017.

[11] A. Crooks, K. Schechtner, A. K. Dey, and A. Hudson-Smith, "Creating Smart Buildings and Cities," *IEEE Pervasive Comput.*, vol. 16, no. 2, pp. 23–25, 2017.

[12] W. Van Raemdonck, T. Van Cutsem, K. S. Esmaili, M. Cortes, P. Dobbelaere, L. Hoste, E. Philips, M. Roelands, and L. Trappeniers, "Building Connected Car Applications on Top of the World-Wide Streams Platform: Demo," in *Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems*, 2017, pp. 315–318.

[13] S. R. Shakeel, J. Takala, and L.-D. Zhu, "Commercialization of renewable energy technologies: A ladder building approach," *Renew. Sustain. Energy Rev.*, vol. 78, no. C, pp. 855–867, 2017.

[14] http://www.hhnmag.com/articles/3438-how-the-internet-of-things-will-affect-health-care,June 2015 (last Accessed: 10 June 2017).

[15] http://www.healthdata.org/pakistan, 2016 (last access 25 November 2017).

[16] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[17] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain," *J. Commun.*, vol. 12, no. 4, 2017.

[18] https://www.forbes.com/sites/reenitadas/2017/05/22/10-ways-internet-of-medical-things-is-revolutionizing-senior-care/#2fa999b5c8f4, MAY 2017 (last Accessed 10 June 2017).

[19] https://www.gartner.com/newsroom/id/3598917, February 2017 (last accessed 10 October 2017)

[20] https://healthinformatics.uic.edu/resources/articles/confidentiality-privacy-and-security-of-health-information-balancing-interests/, December 2014 (last Accessed 10 June 2017).

[21] D. Lake, R. M. R. Milito, M. Morrow, and R. Vargheese, "Internet of things: Architectural framework for ehealth security," J. ICT Stand., vol. 1, no. 3, pp. 301–328, 2014.

[22] https://www.owasp.org/index.php/Main_Page,2017 (last access 2 November 2015)

[23] https://www.cgi.com/sites/default/files/white-papers/cgi-cybersecurity-for-health-data-white-paper.pdf, 2017 (last access 2 june 2015)

[24] L. Yehia, A. Khedr, and A. Darwish, "Hybrid security techniques for Internet of Things healthcare applications," *Adv. Internet Things*, vol. 5, no. 3, p. 21, 2015.

[25] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," arXivPrepr. arXiv1704.08688, 2017.

[26] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," in Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings, M. Joye and J.-J. Quisquater, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 357–370.

[27] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "M2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags," in Ubiquitous Intelligence and Computing: Third International Conference, UIC 2006, Wuhan, China, September 3-6, 2006. Proceedings, J. Ma, H. Jin, L. T. Yang, and J. J.-P. Tsai, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 912–923.

[28] M. Jung, H. Fiedler, and R. Lerch, "8-bit microcontroller system with area efficient AES coprocessor for transponder applications," in Ecrypt workshop on RFID and Lightweight Crypto, 2005, pp. 32–43.

[29] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-chain based forward-secure privacy protection scheme for low-cost RFID," in Proceedings of the SCIS, 2004, vol. 2004, pp. 719–724.

[30] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in Security in pervasive computing, Springer, 2004, pp. 201–212.

[31] D. Molnar and D. Wagner, "Privacy and Security in Library RFID: Issues, Practices, and Architectures," in Proceedings of the 11th ACM Conference on Computer and Communications Security, 2004, pp. 210–219.

[32] P. Dusart and S. Traoré, "Lightweight Authentication Protocol for Low-Cost RFID Tags," in Information Security Theory and Practice. Security of Mobile and Cyber-Physical Systems: 7th IFIP WG 11.2 International Workshop, WISTP 2013, Heraklion, Greece, May 28-30, 2013. Proceedings, L. Cavallaro and D. Gollmann, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 129–144.

[33] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "RFID Systems: A Survey on Security Threats and Proposed Solutions," in Personal Wireless Communications: IFIP TC6 11th International Conference, PWC 2006, Albacete, Spain, September 20-22, 2006. Proceedings, P. Cuenca and L. Orozco-Barbosa, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 159–170.

[34] J. Daemen and V. Rijmen, The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.

[35] M. Katagi and S. Moriai, "Lightweight cryptography for the internet of things," Sony Corp., pp. 7–10, 2008.

[36] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA," in FSE, 2007, vol. 4593, pp. 181–195.

[37] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," in CHES, 2007, vol. 4727, pp. 450–466.

[38] YoHan Park, KiSung Park, KyungKeun Lee, Hwangjun Songand YoungHo Park,Security analysis and enhancements of an improved multi-factor biometric authentication scheme,International Journal of Distributed Sensor Networks 2017, Vol. 13(8)