Authentication of Energy Constrained Devices in Internet of Things based Healthcare System

R. Shantha Mary Joshitta
St. Joseph's College
Tiruchirappalli, Tamil Nadu, India

L. Arockiam
St. Joseph's College
Tiruchirappalli, Tamil Nadu, India

***Abstract*- Internet of things is the prelude to new technological innovation. It expands with different applications such as smart home, smart city, smart grids, smart car, smart healthcare and smart retail. The application of IoT in Healthcare system brings high value for the elderly, victims of chronic disease and those who require constant supervision. But there are many security issues in such application. Moreover, the medical devices used in the IoT enabled Healthcare System are resource constrained devices. So, this paper proposes a novel mechanism for authenticating such resource constrained medical devices. New algorithm for secure authentication and key agreement of the medical devices is also presented. This mechanism is resistance against various security attacks such as eavesdropping, man-in-the-middle and Denial of Service attacks. Formal security analysis and the comparative study presented in this paper have proved that the proposed mechanism has many security features and highly secure among the already existing authentication mechanisms.**

Keywords- Internet of Things, Authentication, Healthcare System, Electronic Product code, Security Metrics, Resource Constraint Devices.

1. INTRODUCTION

Internet of Things (IoT) is a new paradigm where everyday objects are equipped with identifying, sensing and processing capabilities. These objects communicate with one another over the Internet. This enables numerous applications varying from the micro to the macro and from the trivial to the critical. IoT has great impact in all domains. It creates an opportunity for improving efficiency, accuracy and economic benefits in these domains.

Now-a-days, healthcare industry is growing enormously due to the changes in life style and food habit. Healthcare service becomes an issue because of less expert doctors to the people who live in remote villages. To resolve this and make healthcare accessible to all, there is a need for a paradigm shift from stability to mobility. Because of the nature of the IoT environment, there are many issues in the IoT enabled Healthcare System related to secure accumulation, transmission, storage and usage of data. Ensuring ample security in IoT enabled healthcare system is a herculean task. On the other hand, the sources of data themselves need to be secured and authenticated for the medical stakeholders. Security of IoT devices in a healthcare domain is more important, as the data source must be trustworthy to provide proper treatment to the patients. Thus, this paper presents a device authentication mechanism for the IoT enabled healthcare system.

2. RELATED WORKS

Abhishek Sinha et al. presented a secure Key Exchange architecture for the Healthcare Monitoring Sensor Networks (HMSNs) (Abhishek Sinha, Chander Prabha, 2016). It enabled a comprehensive, trustworthy, user-verifiable and cost-effective key management. The proposed architecture protected the entire life cycle of cryptographic keys and allowed only authorized application users to use the keys. The authors used the corporate key management technique for the HMSNs by making it energy efficient. In addition, the authors improved the work with less computational power.

Anitha Chepuru et al. analyzed various security attacks in the existing Intelligent Transportation System (ITS) for the vehicle to vehicle Integration in IoT (Anitha Chepuru, Venugopal Rao K, 2015). The problems in existing IoT were outlined and the authors proposed ECGDSA algorithm for enhancing safety in the vehicle to vehicle system in ITS structure. The algorithm overcame the communication overhead problem in the IKEV2 system. The proposed ECGDSA algorithm was implemented and analyzed in the vehicle to vehicle transportation system.

Byung Mun Lee suggested a binding protocol for public medical devices (Byung Mun Lee, 2015). The proposed protocol provided customized real-time transmission function which enabled interwork between mobile phones, medical devices and monitoring service. The protocol was designed to support streaming date transmission. The operating effectiveness of the protocol was verified by measuring the transmission time.

Debiao He et al. reviewed a recent Anonymous Authentication (AA) scheme for WBANs and pointed out its vulnerability to impersonation attack (Debiao He, Sherali Zeadally, Neeraj Kumar and Jong-Hyouk Lee, 2016). A new AA scheme for WBANs was proposed and proved secure. The detailed analysis demonstrated that the proposed AA scheme not only overcame the security weaknesses of the previous schemes but also had the same computation cost at the client's side.

Hamza Khemissa et al. interconnected a sensor node with a remote user in the proposed research (Hamza Khemissa, Djamel Tandjaoui, 2016). The authors presented a new lightweight authentication scheme for the resource constrained environment. The scheme allowed both the sensor and the remote user to authenticate each other for securely communicating messages. It used exclusive-OR operation, and Keyed-Hash message authentication to check the integrity of the exchanges. The proposed method provided authentication with less energy consumption, and it was terminated with a session key agreement between the sensor node and the remote user. The performance and security analysis were carried out for the proposed scheme. The results showed that the scheme saved energy, and provided resistance against different attacks.

Jun-Ya Lee et al. proposed an encryption method based on XOR manipulation, instead of encryption (Jun-Ya Lee, Wei-Cheng Lin and Yu-Hung Huang, 2014). The authors focused on efficient secure key establishment for the IoT network, used the hash function for privacy protection and anti-counterfeiting. The security was enhanced and hardware design was also demonstrated.

Kritika et al. reviewed the authentication based security model for IoT (Kritika, Harjit Pal Singh, Er. Narinder Pal Singh and Er. Mamta, 2016). The authors stated that several existing authentication schemes were not capable of securing the Internet of Things up to the mark. The authors proved the weakness of XOR manipulation with other 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 proposed another robust method for secure authentication scheme.

Security Management was given much importance and encryption algorithms were considered as one of the best mean for less energy consumption in the research of Santiago et al. (S. Santiago and L. Arockiam, 2016). The researchers outlined the security impacts on energy consumption in order to perform the encryption and decryption functions. Moreover, the authors highlighted the need for the lightweight cryptographic algorithms for the resource-restricted devices. They presented an outline of energy efficiency in IoT environment. The authors pointed out the issues and summarised the ways for minimizing the energy consumption in the IoT environment.

S.M. Joshitta et al. presented the existing works in authenticating the IoT devices (Shantha Mary Joshitta R and Dr. L. Arockiam, 2016). A new architecture and an authentication scheme for smart healthcare system were proposed. The workflow of the system also presented in the paper. Different phases of authentication such as registration, authentication, authorization and key agreement were detailed and working mythology was elaborated by the researchers.

Byung Mun Lee proposed an open healthcare platform structure design and suggested an authenticated registration process (Byung Mun Lee, 2015). The proposed platform linked a mobile device with convenient registration and shared diverse types of medical devices and service. Furthermore, the authors introduced and implemented a health IoT-based mobile application for verifying the efficiency of the proposed method. The above said research contributed user authentication and platform development for IoT-based medical devices.

3. DESIGN GOALS

The aim of this paper is to propose a novel device authentication mechanism for accessing resource-constrained medical devices in smart healthcare environment. Therefore, the following goals should be guaranteed in the proposed authentication of the Medical Devices (MD). The security requirements include:

(a) Secure medical device authentication and key agreement
(b) Resistance to various attacks

To obtain goal (a) all the medical devices used in the system must be authenticated by the Authentication Server (AS). After successful authentication, the secure communication channel should be established between the medical devices and the authentication server. For goal (b) medical devices should be resilient to the security attacks such as man-in-the middle attack, redirect, eavesdropping, impersonation and replay attacks.

4. PROPOSED METHODOLOGY

There are three major phases namely Registration, Login and Authentication in the authentication process of the proposed mechanism. These phases will be explained in the following sessions. For better understanding, the notations used in the proposed mechanism are depicted in Table 1.

Table 1. Notations used in the Proposed Mechanism

Notation	Explanation
MD_i	Medical Device
AS_i	Authentication Server
MS_i	Medical Server
CID_i	Citizen Unique Identification Number
$MCID_i$	Modified CID
PW_i	Password selected by the Patienti
h(.)	Modified Neeva – lightweight One way hash function (Khushboo Bussi, Dhananjoy Dey, Manoj Kumar and B.K. Dass, 2016)
Y_i	Secrete Code for the Patienti
X_i	Intermediate variable in the Patient Registration Phase
EAS[.]	Encryption using Simeck lightweight block cipher (Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, & Guang Gong, Tim Güneysu & Helena Handschuh (Eds.), , 2015)
D[.]	Decryption function using (Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, & Guang Gong, Tim Güneysu & Helena Handschuh (Eds.), , 2015)
IP_i	IP Address of the medical device i
EPC_i	Electronic Product Code of the medical devicei
$MEPC_i$	Modified EPC calculated with nonce M
$\|\|$	Concatenation Operation
$\oplus$	XOR Operation
M^1_i	Modified nonce value selected by the Medical Device i
M_i	Random nonce value generated by the Medical Device i
EPC_Digesti	EPC Digest computed from EPC of MDi
SK_i	Session Key for MDi
T_c	Current Time stamp used to check the Session key SKi
T_1	Time stamp of the Authentication Server
ΔT	Time interval for the allowed transmission delay
F(.)	Left shift operation
F'(.)	Right shift operation
ACK	Acknowledgement sent by the AS after completing Registration of the Patient/Medical Device
Pat_Reg_Tab	Patient Registration Table
Dev_Reg_Tab	Medical Device Registration Table
Pat_Dev_Tab	Patient Device Mapping Table

4.1. Registration Phase

The registration phase is divided into two parts, the patient registration and medical device registration since different inputs and different techniques are used. The registration process runs after the installation of the

medical devices. It is a one-time process and normally carried out by the Authentication Server. There are two important inputs used in the proposed mechanism. They are explained below:

a) Citizen Identification Number (CID): It is a proposed unique identification number for every human on the global. It can be Aadhaar number in India, Social Status Number (SSN) in USA and National Identification Number (NIN) in many other African countries.

b) Electronic Product Code (EPC): This is a 96-bit number, designed as a worldwide identifier that offers a unique identity for every physical object anywhere in the globe.

4.1.1. Patient (P) Registration

- Patient Pi enters his / her CIDi and Password PWi and computes a modified CID. MCIDi= EAS[CIDi || PWi]
- Pi sends MCIDi to the AS for registration
- After receiving the message from Pi, AS computes Xi=DAS[EAS[MCIDi]], CIDi=substring (Xi,0,96)
- AS computes secret code for the Patient Pi Yi=h(Xi)
- AS sends CIDi, PWi, Yi to the Pat_Reg_Tab and sends ACKi to Pi.

4.1.2. Medical Device (MD) Registration

- Medical Device MDi generates a random nonce Mi and computes MEPCi=EPCi ⊕ Mi
- MDi modifies Mi, Mi^1 = F(Mi) and sends MEPCi, Mi^1, IPi for registration
- After receiving the message from MDi, the AS computes Mi using F^1. $Mi=F^1(Mi^1)$
- EPCi=MEPCi ⊕ Mi and EPC_Digesti=h(EPCi || IPi)
- AS sends EPCi, IPi, EPC_Digesti to the Dev_Reg_Tab and sends ACKi to MDi.

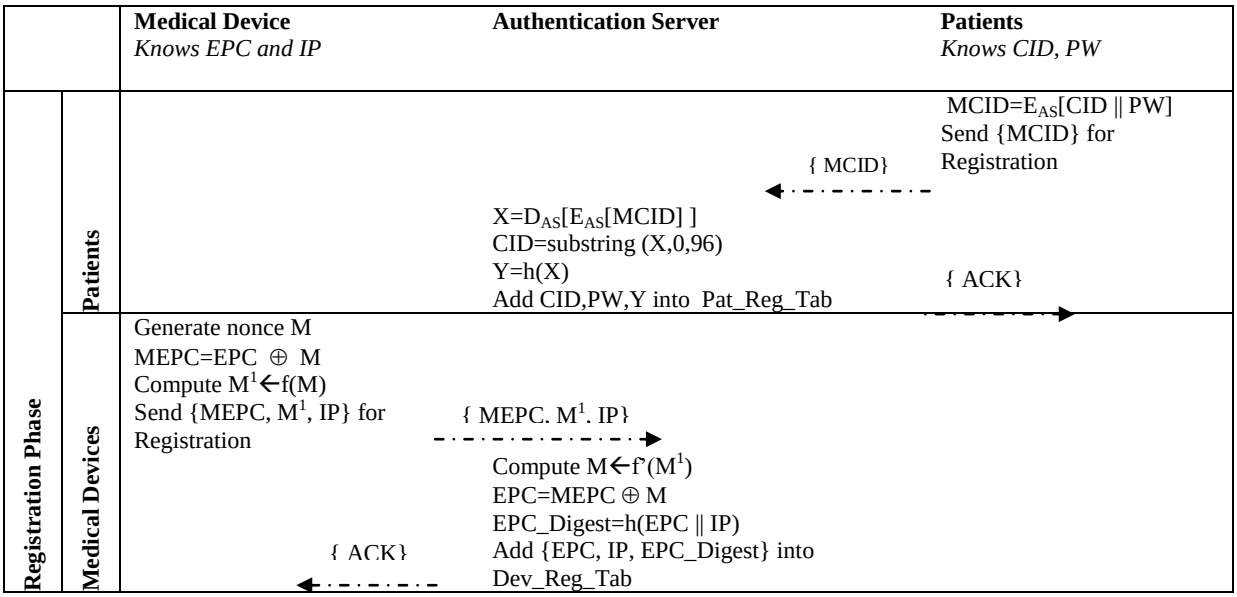

Figure 1. The Registration Phase

The registration process is given in Figure. 1. The sequence diagram of the registration phase of the proposed Mechanism is presented in Figure. 2.

4.2. Login and Authentication Phase

Before authentication starts, the patients and the medical devices have to login for checking the legitimacy of the user. If the verification holds success, it proceeds further to the authentication phase. Otherwise, it forwards the login request to the registration phase and an authentication failed message is sent to the patient or to the medical device.

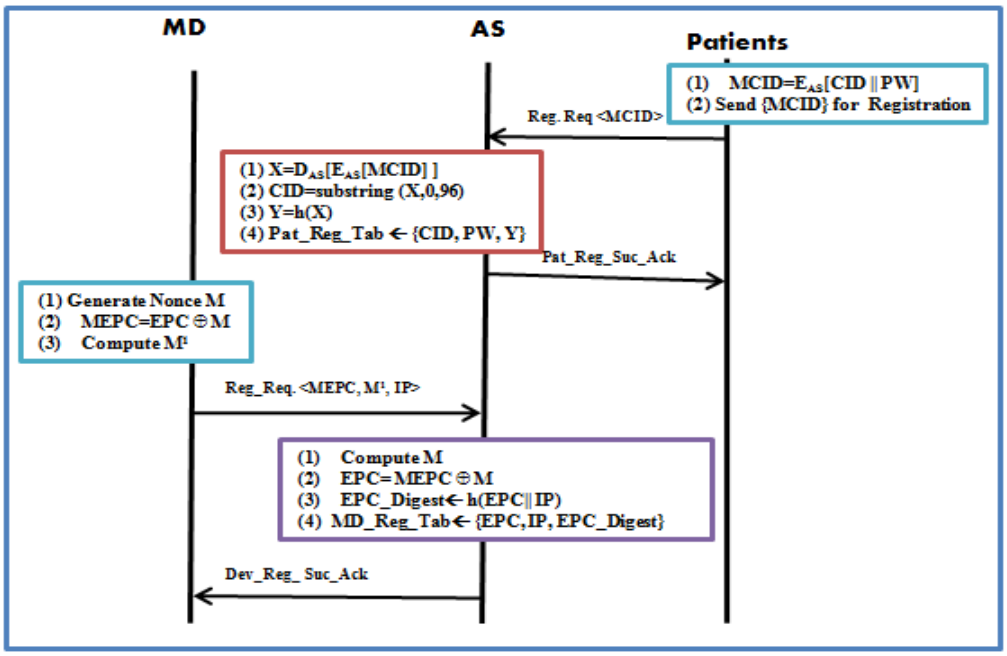

Figure 2. Sequence Diagram of the Registration

4.2.1. Patient Login and Authentication

- Patient P_i login using his / her CID_i and PW_i and computes $MCID_i = E_{AS}[CID_i \| PW_i]$
- Patient P_i sends $MCID_i$ to the AS for login
- After receiving the message from P_i, the AS computes $X_i = D_{AS}[E_{AS}[MCID_i]]$, CID_i=substring (X_i,0,96) and $Y_i = h(X_i)$
- AS validates whether Y_i is equal to the stored Y_i in the Pat_Reg_Tab. If validation occurs, AS sends the secret code Y_i as an authentication message.
- If validation does not hold, the AS forwards the login request to the Registration Phase.

The Login and Authentication phase of the proposed Mechanism is presented in Figure 3-5

	Authentication Server	**Patient** ***Knows CID and PW***
Login Phase		$MCID=E_{AS}[CID \| PW]$ Send 'MCID} for Login {MCID} ◄- - - - - - - -
Authentication Phase	$X=D_{AS}[E_{AS}[MCID]]$ CID=substring (X,0,96) Y=h(X) Check Y into Pat_Reg_Tab If Present, Send Y to Patient Else go to Registration Phase end if	{ Y_i } - - - - - - - - ►

Figure 3. The Login and Authentication phase of the Patient

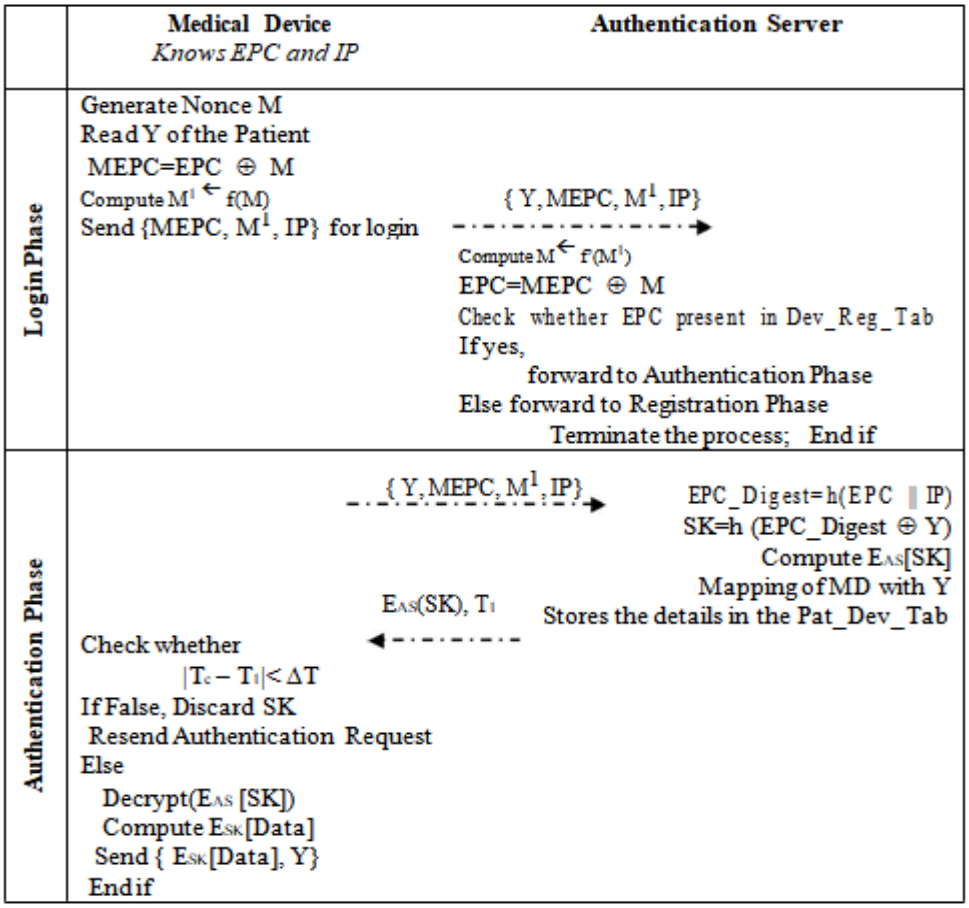

Figure 4. The Login and Authentication Phases of the Medical Device

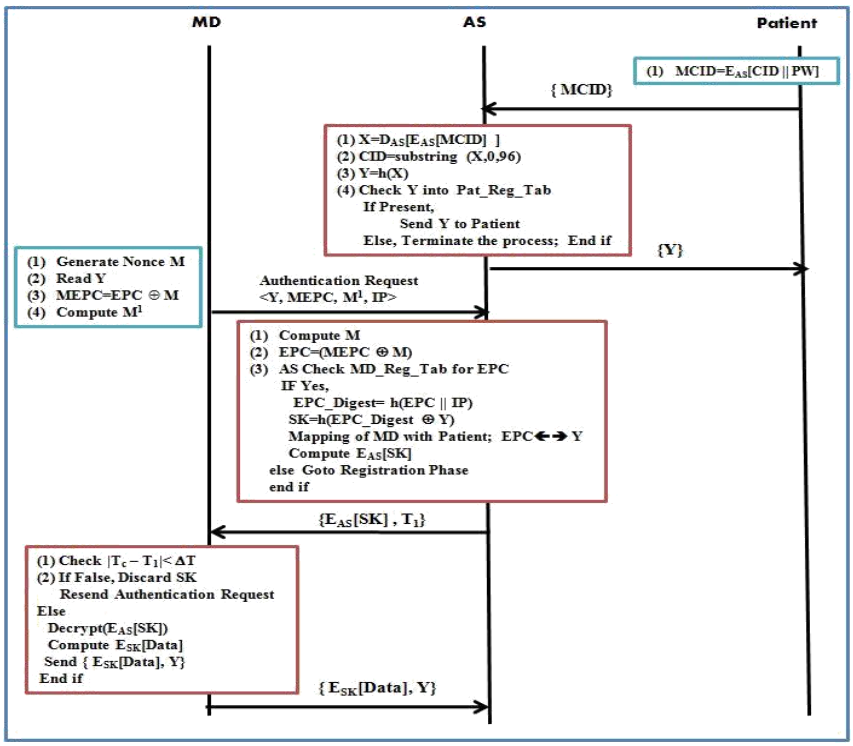

Figure 5. The Sequence Diagram of the Login and Authentication Phase

Table 2. Algorithm Dev_Auth

Input: Patient Details / Medical Device Details

Process:

1. Select name of the Phase; Ch <- {Reg, Login}
2. If(Ch = 'Reg') then
3. Select Type of Registration; Tp <- {Pat, MD}
4. If (Tp = 'Pat') then
5. P_i enter {CID_i, PW_i}
6. Compute $MCID_i = E_{AS}[CID_i \| PW_i]$
7. Call Pat_Reg($MCID_i$)
8. Else
9. Generate nonce M_i
11. Compute M_i^1 <- f(M)
12. Call MD_Reg ($MEPC_i$, M_i^1, IP_i)
13. End if
14. Else
15. Select Type of Login; Tp1{Pat, MD}
16. If (Tp1 = 'Pat') then
17. Enter {CID_i , PW_i }
18. Compute $MCID_i = E_{AS}[CID_i \| PW_i]$
19. Call Pat_login ($MCID_i$)
20. Else
21. MD_i generate random nonce M_i
22. MD_i read Y_i of the Patient P_i
23. MD_i compute $MEPC_i = EPC_iM_i$
24. MD_i compute M_i^1 <- f(M)
25. Call MD_login (Y_i, $MEPC_i$, M_i^1, IP_i)
26. Call MD_Datasent ($E_{AS}[SK_i]$,T_1)
27. End if
28. End if
29. Function Pat_ Reg ($MCID_i$)
30. Compute $X_i = D_{AS}[E_{AS}[MCID_i]]$
31. Compute CID_i=substring (X_i,0,96)
32. $Y_i=h(X_i)$
33. Pat_Reg_Tab <-{CID_i, PW_i, Y_i }
34. Return (ACK_i)
35. End
36. Function MD_Reg ($MEPC_i$, M_i^1, IP_i)
37. Compute $M_i \leftarrow f'(M^1)$
38. Compute $EPC_i=MEPC_{ii}$
39. Compute $EPC\_Digest_i=h(EPC_i \| IP_i)$
40. Dev_Reg_Tab <- {EPC_i, IP_i, EPC_Digest_i}
41. Return (ACK_i)
42. End
43. Function Pat_login ($MCID_i$)
44. Compute $X_i = D_{AS}[E_{AS}[MCID_i]]$
45. Compute CID_i=substring (X_i,0,96)
46. Compute $Y_i=h(X_i)$

If (Y_i = Pat_Reg_Tab (Y_i)) then
  Return (Y_i)
Else
  Return (Auth. Failed Message)
  Terminate the Process
End if
End

Function MD_login ($MEPC_i$, M_i^1, IP_i)
Compute M_i, <- f' (M^1)
Compute EPC_i=$MEPC_i$ | ||
Compute EPC_Digest_i=h(EPC_i || IP_i)
If (EPC = Dev_Reg_Tab (EPC)) then
  Generate EPC_Digest_i = h(EPC_i || IP_i)
  Compute session key $E_{AS}[SK_i]$
  Return ({ $E_{AS}[SK_i]$,T_1})
Else
  Return (Auth. Failed Message)
  Terminate the Process
End if
End

Function MD_Datasent ($E_{AS}[SK_i]$,T_1)
If |Tc – T_1|<-T then
  Decrypt (E_{AS} [SK_i])
  Compute E_{SKi} [$Data_i$]
  Start sending data { $E_{SKi}[Data_i]$,Y_i}
Else
  Discard SK_i
  Resend the Auth. Req.
End if
End

Output: Authentication permission and Session Key

5. RESULT AND DISCUSSION

5.1. Security Analysis

The proposed mechanism is suitable for an insecure IoT enabled healthcare system in which sensitive information may be eavesdropped by a malicious user. The proposed mechanism enables a key agreement, password protection and user anonymity. It created session key SK with time stamp to ensure the freshness of the key and provides enough encryption to secure the communication channel. It is helpful in decreasing the probability of attacks in the proposed mechanism. Moreover, this mechanism provides some advanced features to enhance the security of the mechanism. They are explained below.

- *Data Integrity:* After receiving the session key SK_i from the Authentication Server, a time delay is checked to find the replay attack. If no such attack found, then, it starts sending the medical data it has collected in the last few seconds to the AS which is encrypted by the newly given session key SK_i. When AS receives any information or data from any medical device, it verifies the integrity of the information by checking the secret code of the Patient in the Pat_Dev_Tab. If the verification holds success, then it saves the medical data sent by the medical device MD in the Medical Server (MS) available in the cloud storage and its meta-data is kept in the AS for future reference.

- *Device Identity Protection:* Creation of MEPC and verification of the EPC for every exchange of authentication request will prevent the chances of any theft or alteration in the identity of the medical device. If any new EPC is found, then the mechanism immediately discards the request sent by the particular medical device and forwards it to the registration phase.
- *Session key establishment:* After the successful authentication of any medical device, the generated session key SK will be encrypted using the public key of the AS by the use of Simon and Speck block ciphers by the AS. It acts as a key for the secure communication channel between the two entities of the communication.
- *Scalability:* Scalability is the major issue in the smart healthcare environment. The proposed mechanism is extensible as it permits addition of new medical device into the environment by registering itself. The device details will be added into the Dev_Reg_Tab and mapping of medical device with the patient is performed in the authentication phase of the mechanism.
- *Synchronization free Mechanism:* Creation of time stamp T for every session ensures the freshness of each session. It helps eliminate the replay attack and confirms that the received data are not an old replayed data. Therefore, the proposed mechanism reduces the need for the implementation of synchronization between the participating entities.
- *Forward security:* In the proposed mechanism, it is impossible for any malicious user to correlate any two communication sessions because of the creation of new session key for each session. Moreover, it also cannot receive the previous communication from the ongoing session.
- *Privacy Preservation:* In the proposed mechanism, the medical devices are not communicating among themselves. They are not aware of the individual's private information (e.g., location). So, they will not disclose any private information of the patients.
- *Traceability protection:* In the proposed mechanism, it is not easy to trace the patient or medical device even though anyone knows the CID of the patient and EPC of the MD. Because, at each and every communication request, the secrete key of the Patient and the EPC_Digest of the MD is created and verified in the respective registration tables. If such verification holds, then authentication provides otherwise, the patient and the MD will be forwarded to the registration phase.
- *Password protection:* There is a possibility of intercepting the password of any medical device by an intruder while it would be sent over an insecure channel. The intruder could use it in order to impersonate a legitimate medical device. In the proposed scheme no password exchange is permitted and it is used only in the registration of the patient. So, the probability of stealing or eavesdropping of password is less. The proposed mechanism guarantees password protection in a way that it never uses the password selected by a patient for the authentication process. Moreover, AS never sends any password over any insecure channel.
- *Medical Device anonymity:* Though the medical device communicates with the Authentication Server using its EPC, a part of the EPC is later hashed and used in the proposed mechanism. So, device identity is maintained secretly and it is difficult to identify the device from the session key.

5.2. Attack Resistance of the proposed mechanism

Moreover, it is resilient against replay attacks, privileged insider attacks, impersonation attacks and denial- of-service attacks.

- *Man-in-the-Middle Attack:* The CID of the Patient and EPC of the MD are not communicated directly over the communication channel in the proposed mechanism. They were encrypted or modified to provide security over the communication channel using the Neeva lightweight one way hash function and the encryption algorithm Simon and Speck block ciphers which is specially designed for the Internet of Things (Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks and Louis Wingers, 2015). Moreover, the session key SK is encrypted using the public key of the AS for every exchange of the session key. So, it is impossible for the malicious users who try to steel or overhear any secrete information from the communication channel.
- *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 mechanism, DoS

attack is not possible because the encrypted session key only exchanged after the successful authentication.

- *Eavesdropping:* It is nothing but secretly listening to a conversation / communication between two endpoints without any authorization. Here, in the proposed mechanism, the computed EPC_Digest is not communicated to the medical devices. While any medical device tries to communicate with the AS. The AS immediately computes the EPC from the MEPC 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 T1. Otherwise, communication between the respective devices with the AS is not allowed. So, the possibilities of eavesdropping is restricted or avoided.
- *Impersonation:* It is an act of fantasizing to be another node for the purpose of making fraud. But in the proposed mechanism, every device in the communication path is addressed or accessed not by its IP but by its EPC. This EPC is globally unique and no patient secrete code computed at the registration phase is communicated between MD and the AS. So, the proposed mechanism reduces the impersonation attack.
- *Replay Attack:* It is a playback attack where the valid data communication is fraudulently repeated or delayed. If any intruder captures the session key SK between MD and the AS, he may replay it to impersonate the MD. It is very dangerous in the healthcare scenario. To overcome this attack, Time Stamp T1 is used along with the authentication information. The delay in the time stamp T1 is calculated for every exchange of session key. If the delay is within the threshold time (ΔT) then data transfer starts. Otherwise, the session key SK is discarded and new authentication process is initiated.
- *Redirection Attack:* In any communication channel, the probability of collecting the private information of the user by a malicious user is high. The malicious user may impersonate any medical device and reprogram it to forward the user's medical data to another destination. But in the proposed mechanism, the attacker cannot entrap the medical device, because it connects itself with the AS with its EPC not by its IP. IP spoofing is very easy whereas tracking of EPC is not so. Moreover, the entire EPC of the medical device is not used in the proposed mechanism. So, the probability of the redirection attack is less in the mechanism.
- *Privileged-insider attack:* An insider attack is an attack initiated by a privileged but malicious medical device. The malicious MD uses its privileges in order to collect some private information about an intended patient. It can then exploit such private patient information of the patient in order to gain something important. In the proposed mechanism, EMPC is sent from the medical device in the authentication request but for composing session key SK, EPC_Digest is used which is not revealed over any communication channel. Thus, privileged insider attack is avoided.

5.3. Formal Security Analysis

The formal security analysis of the proposed mechanism is presented in this subsection. The hash function is defined as given in [Das AK, 2013].

Definition: $h:\{0,1\}^* \rightarrow \{0,1\}^1$ is a secure one way hash function. It produces a string $h(a) \in \{0,1\}^1$ given an arbitrary binary string $a \in \{0,1\}^*$ as input. The hash function satisfies the following properties:

a) It is computationally infeasible to find $a \in A$ such that $b = h(b)$ where $b \in B$;

b) Given $a \in A$, it is computationally infeasible to find another $a^1 \neq a \in A$ such that $h(a^1) = h(a)$;

c) It is computationally infeasible to find a pair $(a^1, a) \in A^1 \times A$ with $a^1 \neq a$ such that $h(a^1) = h(a)$

Theorem: Let the one-way hash function h(.) normally behaves like an interface. The proposed mechanism is provably secure against any intruder I for the protection of a patient P_i's personal information including the Citizen Identity Number CID_i, password PW_i and the secret number Y_i computed by the AS for a patient P_i and a pre-shared secret key between the AS and P_i.

Proof: The formal security analysis of the proposed mechanism follows the algorithm proposed in [Jongho Moon, Younsung Choi, Jaewook Jung and Dongho Won, 2015]. Let the Intruder I will have the ability to derive

the Citizen Identity Number CID_i, password PW_i and the secret number Y_i computed by the AS for a patient P_i and a pre-shared secret key between the AS and P_i.

Reveal: This random interface will unconditionally output the input a from the given hash result $b = h(a)$.

Now, *I* runs the experimental algorithm presented in $EXP_{HASH,I}$ for the proposed device authentication mechanism.

If the success probability of the experimental algorithm $EXP_{HASH,I}$ is defined as .the advantage function for this experiment then becomes, $Adv_{HASH,I}(t, q_n) = \max_I Success_{HASH,I}$ where the maximum is taken over all of *I* with the execution time *t* and the number of queries q_n that are made to the Reveal interface. Consider the experiment in [Lu YR, Li LX, Yang X and Yang YX, 2015]. If *I* has the ability to solve the hash function problem that is provided in *Definition*, then the intruder *I* can directly derive the Ci tizen Identity Number CID_i, password PW_i and the secret number Y_i computed by the AS for a patient P_i and a pre-shared secret key between the AS and P_i. In this case, *I* will discover the complete connections between P_i and AS; however, it is a computationally infeasible problem to invert the input from a given hash value, i.e., $Adv_{HASH,I}(t) \leq \in, \forall \in > 0$.

Then, we have $Adv_{HASH,I}(t, q_n) \leq \in$, since $Adv_{HASH,I}(t, q_n)$ depends on $Adv_{HASH,I}(t)$. As a result, there is no way for *I* to discover the co mmplete connections between P_i and AS, and, by deriving *(CID_i, PW_i, Y_i, Pre-shared secret key).* Thus, the proposed authentication mechanism is provably secure against an Intruder. Table 3 Presents a comparative study of the security features among the proposed and already existing authentication mechanisms. It also presents a comparison of the mechanism's resilience against various attacks.

Table 3. Comparison of Security features among proposed and other existing schemes

S.No.	Security Metrics	Hamza Scheme	MS Farash Scheme	H Ning Scheme	C Lai Scheme	Proposed mechanism
1.	Mutual authentication	Yes	Yes	No	Yes	No
2.	Key agreement	Yes	Yes	No	Yes	Yes
3.	Traceability protection	No	Yes	No	No	Yes
4.	Password protection	No	Yes	No	No	Yes
5.	Dynamic node addition	Yes	Yes	No	No	Yes
6.	Device anonymity	No	Yes	No	No	Yes
7.	Data Integrity	Yes	No	No	No	Yes
8.	Identity Protection	Yes	No	No	No	Yes
9.	Synchronization Independence	Yes	No	No	No	Yes
10.	Privacy Preservation	No	No	*Yes*	Yes	Yes
11.	Forward Security	No	No	No	Yes	Yes
	Resilience against					
1.	Dictionary Attack	No	No	No	No	Yes
2.	Brute-Force Attack	No	No	No	No	Yes
3.	Replay attack	Yes	Yes	No	No	Yes
4.	Privileged-insider attack	Yes	Yes	No	No	Yes
5.	Man-in-the-middle attack	No	Yes	No	No	Yes
6.	Device impersonation attack	No	Yes	No	No	Yes
7.	DoS attack	Yes	Yes	No	No	Yes
8.	Redirection Attack	No	No	*Yes*	No	Yes
9.	Eavesdropping Attack	No	No	No	No	Yes

5.4. Formal Security Analysis

The formal security analysis of the proposed mechanism is presented in this subsection. The hash function is defined as given in [Das AK, 2013].

Definition: $h:\{0,1\}^* \rightarrow \{0,1\}^1$ is a secure one way hash function. It produces a string $h(a) \in \{0,1\}^1$ given an arbitrary binary string $a \in \{0,1\}^*$ as input. The hash function satisfies the following properties:

a) It is computationally infeasible to find $a \in A$ such that $b = h(b)$ where $b \in B$;

b) Given $a \in A$, it is computationally infeasible to find another $a^1 \neq a \in A$ such that $h(a^1) = h(a)$;

c) It is computationally infeasible to find a pair $(a^1, a) \in A^1 \times A$ with $a^1 \neq a$ such that $h(a^1) = h(a)$

Theorem: Let the one-way hash function h(.) normally behaves like an interface. The proposed mechanism is provably secure against any intruder I for the protection of a patient Pi's personal information including the Citizen Identity Number CIDi, password PWi and the secret number Yi computed by the AS for a patient Pi and a pre-shared secret key between the AS and Pi.

Proof: The formal security analysis of the proposed mechanism follows the algorithm proposed in [Jongho Moon, Younsung Choi, Jaewook Jung and Dongho Won, 2015]. Let the Intruder I will have the ability to derive the Citizen Identity Number CIDi, password PWi and the secret number Yi computed by the AS for a patient Pi and a pre-shared secret key between the AS and Pi.

Reveal: This random interface will unconditionally output the input a from the given hash result b □ h □a □ .

Now, I runs the experimental algorithm presented in [13] EXPHASH , I for the proposed device authentication mechanism.

If the success probability of the experimental algorithm EXPHASH, I is defined as .the advantage function for this experiment then becomes, where the maximum is taken over all of I with the execution time t and the number of queries qn that are made to the Reveal interface. Consider the experiment in [Lu YR, Li LX, Yang X and Yang YX, 2015]. If I has the ability to solve the hash function problem that is provided in Definition, then the intruder I can directly derive the Ci tizen Identity Number CIDi, password PWi and the secret number Yi computed by the AS for a patient Pi and a pre-shared secret key between the AS and Pi. In this case, I will discover the complete connections between Pi and AS; however, it is a AdvHASH ,I t. As a result, there is no way for I to discover the co mmplete connections between Pi and AS, and, by deriving (CIDi, PWi, Yi, Pre-shared secret key). Thus, the proposed authentication mechanism is provably secure against an Intruder.

6. CONCLUSION

A secure device authentication mechanism for IoT enabled healthcare system is presented in this paper. The proposed authentication mechanism uses EPC of the medical devices and modified Neeva one way hash function to check the integrity of the medical information communicated. It helps to reduce the probability of the attacker taking advantage of a forged EPC of the MD. An algorithm for registration and authentication of the patients and medical devices is proposed and formal security analysis is performed. Moreover, a comparative study of the security features among proposed and other existing schemes is also presented. The formal security analysis explicitly proved that the proposed mechanism is suitable for any insecure IoT smart healthcare environment.

REFERENCES

Abhishek Sinha, & Chander Prabha (2016). Multi-level authentication for Internet of Things for Secure healthcare network establishment. International Journal of Modern Computer Science (IJMCS), 4(2), 90-93.

Das, A. K. (2013). A secure & effective user authentication and privacy preserving protocol with smart cards.Networking Science, 2(1-2), 12-27.

Anitha Chepuru & Venugopal Rao, K. (2015). Performance Analysis of RFID Authentication in Intelligent. International Journal of Emerging Technology and, 5 (12),, 144-150.

Shantha Mary Joshitta, R. & Arockiam, L. (2016). A Neoteric Authentication Scheme for IoT Healthcare System. International Journal of Engineering Sciences & Research Technology, 5(12), 296-303.

Santiago, S. & Arockiam L. (2016). Energy Efficiency in Internet of Things: An Overview. International Journal of Recent Trends in Engineering & Research (IJRTER), 2(6), 475-482.

Debiao He, Sherali Zeadally, Neeraj Kumar & Jong-Hyouk Lee (2016). Anonymous Authentication for Wireless Body Area Networks With Provable Security. IEEE Systems Journal, 99, 1-12.

Hamza Khemissa & Djamel Tandjaoui (2016). A Novel Lightweight Authentication Scheme for heterogeneous Wireless Sensor Networks in the context of Internet of Things. 15th Annual Wireless Telecommunications Symposium.

Jongho Moon, Younsung Choi, Jaewook Jung & Dongho Won (2015). An Improvement of Robust Biometrics-Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards. PLoS ONE, 10 (12), 1-15.

Jun-Ya Lee, Wei-Cheng Lin & Yu-Hung Huang (2014). A Lightweight Authentication Protocol for Internet of Things. International Symposium on Next-Generation Electronics (ISNE).

Kritika, Harjit Pal Singh, Narinder Pal Singh & Mamta (2016). Multivariate Authentication. Imperial Journal of Interdisciplinary Research (IJIR), 2(8), 543-550.

Lee, B. (2015). Registration Protocol for Health IoT Platform to Share the Use of Medical Devices.

International Journal of Bio-Science and Bio-Technology, 7(4), 1-10.

Lee, B. (2015). Dynamic Data Binding Protocol between IoT Medical Device and IoT Medical. International Journal of Smart Home, 9 (6), 141-150.

Lu, Y.R., Li, L.X., Yang, X. & Yang, Y.X.. (2015). Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards. PLoS One, 10 (5), 1-15.