International Conference on Advances in Materials, Computing and Communication Technologies
In Association withInternational Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Lightweight Solutions for Securing IoT Based Healthcare System

Ms. P. Jeyadurga[1], Dr. S. Ebenezer Juliet[2]

[1]Assistant Professor, Department of Computer Science and Engineering, Dr. Sivanthi Aditanar College of Engineering, Tiruchendur, Tamil Nadu, India

[2]Associate Professor, Department of Computer Science and Engineering, VV College of Engineering, Tisaiyanvilai, Tamil Nadu, India

ABSTRACT

Internet of Things (IoT) is an emerging field that plays a vital role in medical application. The Wireless Body Sensor Network (WBSN) technology is integrated with IoT for an efficient healthcare monitoring. In this system, wearable wireless body sensors are used on patient's body to monitor their heath condition and report to concerned care takers in case of any emergency situation, when a patient's life is under risk. IoT introduces new challenges for the security of the system and the proposed protocol aims at enhancing security in IoT based automated modern healthcare system. As security is one of the major mandatory requirements of healthcare application, a strict authentication scheme must be developed to ensure patient's privacy by preventing critical information from eavesdropping. To overcome the security threats in the existing healthcare system, a novel approach is introduced to provide lightweight solutions. The proposed lightweight anonymous authentication protocol is useful in many IoT applications where security is a major concern. The security analysis shows that this system satisfies all the essential security requirements and withstands all the possible attacks to give advanced healthcare support. The communication and computation overhead is reduced by employing the proposed lightweight authentication protocol. The comparative results demonstrate that the proposed protocol is efficient and robust than the existing protocols.

KEYWORDS - Internet of Things, Wireless Body Sensor Network, HealthCare, Security, Hash function, Mutual Authentication.

I. INTRODUCTION

The World Wide Web (WWW) which is introduced in the year 1991 allowed the internet to gain its popularity. Internet allows people to communicate with each other whereas Internet of Things (IoT) is all about connecting devices around us. This can be accomplished using sensors and actuators. Today the world has deployed around 5 billion smart devices and it will ascend to 50 billion by 2020 as indicated by predictions [1]. The top most application of IoT includes traffic monitoring, Healthcare monitoring, security, transport and logistics. IoT picked up popularity in healthcare industries as it introduces automation which permits individuals to live a sophisticated lifestyle.

According to the report by World Health Organization (WHO), the population of old people will be around 1.5 billion by 2050[2]. This expansion in the number of aged people leads to an increasing demand on healthcare system. Since one half of the senior people are affected by chronic diseases such as Blood Pressure (BP), diabetics, asthma etc., they find it hard to accomplish their everyday tasks without the help of caretakers. The advanced healthcare solution supports senior individuals to live a decent life style.

Wireless sensor technology is utilized as a part of numerous applications such as traffic control system, healthcare industries and so forth. In Wireless Body Sensor Network (WBSN) technology, Smart wearable body sensors can be used on bodies to monitor the health of an individual. Due to the involvement of WBSN technology, the healthcare industries gained huge importance in 21st century [3]. This technology is integrated with IoT to offer medical services to individuals by an application server with the help of the application in smart gadget. This offers an efficient healthcare monitoring. However, deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable. Since, the physiological data of an individual are highly sensitive, security is a vital requirement of healthcare applications.

Cryptography provides the foundation to achieve necessary security goals in networks. Lightweight Cryptography (LWC) is a cryptographic algorithm or protocol [4] designed for implementation in constrained environments such as smart healthcare devices, RFID tags, sensors and so on. Chip size and energy consumption are the key measures to evaluate the lightweight properties in hardware implementation whereas in software implementation, it is evaluated by the code and RAM size. Lightweight cryptography provides sufficient security and it is used in IoT to achieve efficiency of end-to-end communication and for applicability to lower resource devices. The proposed lightweight authentication system for smart health uses hash based computation, random nonce generation, time stamp generation, Bitwise Exclusive OR operation and Concatenation operation to enhance the security of messages exchanged between mobile unit and healthcare server. Many cryptography schemes have been studied and their speed performance is compared [5]. It is found that SHA-256 is faster with 31% than SHA-512 when hashing small strings. So the proposed protocol utilizes SHA-256 hashing technique.

In this paper, we proposed WBSN based healthcare system offers advanced healthcare support to senior people in a secured way. Our protocol significantly reduces the overhead when compared with other approaches. In this paper, section 2 describes the literature review of previous works. Section 3 presents the methodology of the proposed work. The performance and security analysis is discussed in section 4. The simulation result is shown in section 5. Finally, conclusion is given in section V.

II. RELATED WORKS

The increase in population, unbalanced resource utilization, declining birth rate, etc., leads to some social problems that become obvious in the healthcare field. The inability of responding to emergency and inadequate early detection and prevention capability are the major issues in healthcare sector. Several healthcare projects based on IoT has been developed that made patient monitoring more beneficial. In 2006, Alarm-net [6] is developed that utilized real time queries to interact with the system and to collect data automatically. The security of the medical records is ensured by encrypting the communication channel with AES. However, this scheme is susceptible to confidentiality attack that leads to leakage of the location information. The authors of paper [7] suggests the use of fuzzy-rule scheduling

algorithm and radio activation policy to meet the requirements under unrealistic medical settings. The research in [8] and [9] utilizes various cryptographic algorithms such as AES and Diffie-Hellman respectively for encrypting the data transmission over network. The schemes presented in [10], [11] and [12] successfully implemented the healthcare monitoring system using hardware but these models doesn't provide solutions to any of the security requirements like anonymity, secure localization etc., that are essential for a secure patient monitoring system. Zhaoyang Zhang et al.[13] proposed ECG-IJS algorithm which used ECG signal as a biometric for key generation. This key is then used for further data encryption and hash-based message authentication. The security analysis hasn't focussed on attack resistance property. A novel security scheme is designed by the authors [14] to facilitate security to medical data. This design combines signature and encryption which provides both security and authentication for BANs. It also includes error tolerance capability. Some studies [15] and [16] have shown that it satisfies all the necessary security requirements and resilient against strong attacks. Lightweight anonymous authentication protocol using k-pseudonym set is presented by the authors [17]. This scheme is highly efficient and flexible. However the overhead of the system depends on the construction of k- pseudonym set. Next in 2015, Chunhua Jin et.al. demonstrated [18] a new RFID model which is highly suitable for healthcare environment and the RFID authentication protocol ensures secure communication over network. This model could withstand several security attacks but communication cost is high. The research in [19,20,21,22,23] employed low cost cryptographic primitives such as one-way hash function and Exclusive OR operation in the authentication protocol to satisfy all the security requirements and to reduce the overheads. However the schemes presented in [22] and [23] failed to include the GPS information which allows detecting location of chronic patient.

The research work presented in [24] provides a Secure and Anonymous Biometric Based User Authentication Scheme (SAB-UAS) to ensure secure communication in healthcare applications. The random-oracle model is provided to show security efficiencies in medical application systems. The system used NS3 simulator for experimental analysis of network parameters. However, SAB-UAS scheme experiences more congestion when the number of message transmission increases proportionally. Li, Xiong, et al. [25] proposed an ECC based secure three-factor authentication protocol with forward secrecy for WMSN. It utilized a fuzzy commitment scheme and honey_list techniques to handle the biometric information and to solve mobile device lost attack respectively. The result shows that the Communication cost (2720 bits) is quite high. Zhang et al. [26] introduced PASH, a privacy-aware s-health access control system, in which the key ingredient is a large universe CP-ABE with access policies partially hidden. In PASH, attribute values of access policies are hidden in encrypted SHRs and only attribute names are shown. however, they failed to focus on few security factors and traceability mechanisms which is crucial. Wang et al. [27] proposed HeOC scheme in which the authenticated users can send the encrypted physiological data to the cloud and query the specific disease level accurately on the encrypted medical data stored in the cloud. the user queries the diagnosis result accurately with the oblivious pseudorandom function protocol (OPRF). In order to demonstrate the efficiency of computations and communications, an android app and two python programs are used. The test results of computational cost at user side is comparatively higher. To overcome the typical problems found in the existing systems, a new lightweight authentication protocol is proposed to ensure the security of the system and to reduce the overhead.

III. PROPOSED SYSTEM

The system architecture is shown in Figure. 1. The architecture comprises of Wireless Body Sensor Network (WBSN), Mobile Unit (MU), HealthCare Server and Care-takers. The care- takers here include physician, family members and emergency care centre.

WBSN consists of group of sensor nodes that collects physiological data from human body and sends it to the MU via internet or bluetooth. The MU processes the received data and requests the server to send alert messages to the concerned care takers based on the degree of abnormalities, in case of any emergency situation.

Due to highly sensitive applications of the WSNs, an efficient authentication scheme must be designed. The principal goal of this paper is to design a lightweight authenticated anonymous protocol,

- To achieve mutual authentication between MU and server and to achieve security features like anonymity, secure localization, data integrity, data freshness, etc.
- To reduce computation and communication overhead
- Early detection of incorrect entries of user identity or password in order to make login phase efficient
- To resist attacks like replay attack, Eavesdropping attack, Mobile Device Stolen Attack, Session Key Attack, Man-in-the-middle attack and impersonation attack
- To establish session key between the communicating entities

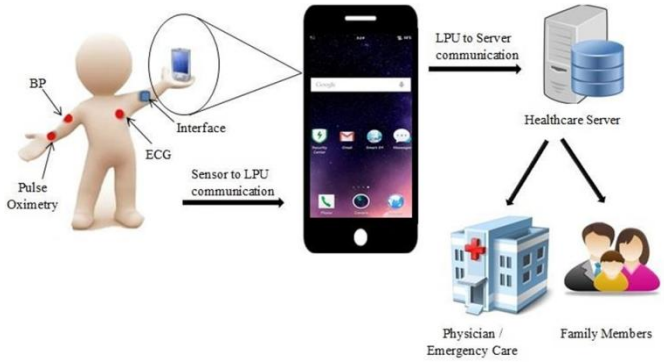

Figure 1. Block Diagram of Proposed System

Modules Description

The proposed system is composed of 3 stages. The first one is the communication between WBSN and MU. The second step is to secure the communication between MU and the server. The final stage is to secure the data stored in the database.

Data from WBSN to MU

In this work, WBSN is intended to monitor patient's Blood Pressure (BP) and body temperature continuously. The MU reads data from the sensors and processes the received data and requests the server to send alert messages to the concerned care takers. Table 1 represents the sample data for BP and temperature for 10 rounds on a timely basis.

At round 2, the BP value is 120/80 which is considered to be normal and therefore no action takes place. At round 3, the value is 160/100 which indicates high BP and at round 8, the value is 80/60 which indicates low BP. For these cases, emergency care is contacted immediately. The sensed value is then processed by an android application that is designed solely for healthcare monitoring. For instance, the body temperature value ranging from 98.4 to 99.6 is normal.

When the Body temperature of the individual crosses this limit, it is taken into consideration as an abnormal level. The device monitors the patient continuously and if the patient's temperature goes above a certain limit, it sends alert messages to the

care takers through the healthcare server. Table 2 shows the action table for BP and temperature data

Table 1. Sample Data from WBSN.

Rounds	Sample Data from WBSN	
	BP data	Temperature data in F
1	130/90	102.6
2	120/80	98
3	160/100	103
4	110/70	101.7
5	120/80	97
6	130/90	98.5
7	100/60	103.6
8	80/60	104
9	130/90	103.2
10	110/70	98

Table 2. Action Table for BP and Temperature Data.

WBSN BP Data	WBSN Temperature Data	Action
BP ⩾ 80 ⩽ 120	Temp ⩾ 98.4 ⩽ 99.6	No action
BP > 130 & BP < 70	Temp > 99.6 & Temp ⩽ 102	Inform family members
BP > 160 & BP < 60	Temp > 102	Inform Emergency care and physician

Communication between MU and Server

The medical data sent from the MU to the server must be secured in order to prevent patient's private information from attackers. The security requirement includes authentication, anonymity, secure localization, and so on. To accomplish all these requirements, cryptographic hash function and Bitwise Exclusive-OR operation are employed in order to achieve lightweight solution that reduces the computation overhead. The various notations that are used in the lightweight authentication protocol are described in Table 3.

Table 3. Notations and Cryptographic functions.

Notations	Description
M	Mobile Unit
S	HealthCare Server
IDL	Identity of the MU
PL	Password of the MU
TS	Time Stamp generated by Server
DL	Message Digest of MU
R1	Random Nonce created by MU
LM	Location of the Mobile Unit
Pid	Pseudo Identity
PP	Pseudo Password
SID	Session ID
RS	Response of the server
h(.)	One-way hash function
⊕	Exclusive-OR operation
||	Concatenation operation

First, the user details need to be registered with the Health Care Server and the security parameters must be obtained. Then the authentication protocol is executed to provide two-factor authentication. Two-Factor Authentication (2FA) is a method in which the user gives two authentication features to confirm their authenticity. It is used to control the access to sensitive data which prevents the users' data from being accessed by hackers.

a) User Registration Phase

To monitor the patient and to get services from an opted server, every new user is required to register their details with the healthcare sever. So the user is required to undergo registration process. The personal details include name, mobile number and mail ID of the patient, family members, physician and emergency care. All these informations are stored in the database of the healthcare server. In the IoT, the HealthCare Server and all the users of the device are expected to be honest in the device registration phase.

R1: In this phase, the user freely selects his/her identity IDL and chooses a password PL of his choice

and submits the registration request to the healthcare sever via secure channel.

R2: Upon receiving the user's registration request, the server verifies IDL. If the IDL is already registered with other user, the server asks for new identity. Otherwise, the server assigns a unique authentication time stamp TS for the user. Only the registered user with the identity IDL and password PL can obtain TS as an authentication token from the Server. TS is randomly generated by the server and it is mainly used to prevent replay attack and to speed up the process. During the execution of anonymous authentication phase, the server checks the TS received from the mobile unit with the one stored in the database. The server will abort the connection if any mismatch found. In that case, the mobile unit will be asked to communicate with the pseudo-identities.

R3: The Server generates a group of unlinkable pseudo-identities PID = {Pid1, Pid2,…}, where Pidi PID and it is computed by Pidi = h(IDL||r||PL). Here r denotes the random number used for deriving pseudo identity. It also produces a group of pseudo passwords PP ={P_{P_1} , P_{P_2} ,…} which corresponds to a particular Pidi. These can be used during loss of synchronization. Once a pair (Pidi,PP) is used for communication, it must be deleted from the list by both parties. Finally the server sends {(Pid,PP),TS,SID} to the MU and keeps a copy in its own database for further communication.

All these calculations are done in the registration phase and the security credits generated during this phase are used for the mutual authentication for providing adequate security for the smart health system. No users and server is trusted after the registration phase is over.

b) Login and Lightweight authentication phase

This phase achieves the goal of mutual authentication between mobile unit and healthcare server. It consists of two steps: MA1 and MA2. MA1 denotes the message authentication between MU and server whereas MA2 represents the message authentication between Server and MU. The description of this phase is described below.

Step 1: The MU inputs the login credentials into the mobile device. Then it computes DL = h (IDL||PL). The identity and password from the MU is hashed using SHA-256 hashing technique.

Step 2: The MU also generates a random nonce R1 and calculates RL=DL⊕R1. Then the MU computes LM = GPS ⊕ DL. It then forms the authentication request with AIDL= h (IDL||PL||R1||TS) and sends the message MA1: {DL, AIDL, LM, RL, TS} to the healthcare server.

In case of loss of synchronization, the mobile unit communicates with the help of the pseudo identity and password i.e., it assigns AIDL = Pid and PL = Pp. In this case, no TS will be sent.

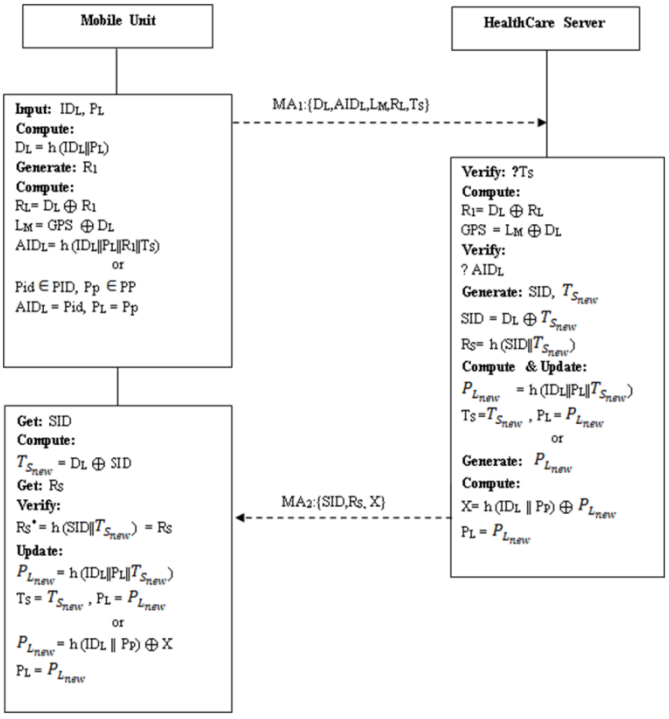

Figure 2. Lightweight Authentication Protocol

Step 3: The Server verifies the timestamp TS. It then retrieves RL from MA1 and computes R1= DL ⊕ RL. Then, it retrieves the location of the mobile unit by computing GPS = LM ⊕ DL. The Server now checks whether the AIDL from MU is valid or not. If it is valid, the message sent by the MU is authentic. Otherwise, the protocol operation is stopped.

Step 4: After verifying the legitimacy of the user, the server generates a session to communicate with the MU. The server also produces $T_{S_{new}}$ which is a random number. The session ID is unique and is computed by SID = DL⊕ $T_{S_{new}}$. A new session is established whenever the server finds a valid request from an authenticated user. The user's information will be safe while the communication takes place in that session. After the log out process, the session gets terminated and cannot be used further for malicious purpose.

Step 5: The server computes the response RS= h (SID|| $T_{S_{new}}$). It then computes $P_{L_{new}}$ = h (IDL||PL|| $T_{S_{new}}$) and updates < TS, PL> with <$T_{S_{new}}$, $P_{L_{new}}$>. This phase periodically updates the old password to a new password. The message MA2:{SID,RS,X} is created by the server and sent to the MU. Here, only the partial hash code of SID is sent to the mobile unit to improve the security.

If there is no TS in MA1, then the server checks the validity and freshness of the AIDL = Pid . If the server cannot find the Pid in AIDL, it terminates the connection. If it finds the Pid, the server will compute new password $P_{L_{new}}$ and then calculates X= h (IDL || PP) ⊕ $P_{L_{new}}$ and sends X along with MA2.

Step 6: After receiving MA2, the mobile unit gets the SID and then computes $T_{S_{new}}$= DL ⊕ SID .It then checks whether R *?=R holds. If it is correct, the mobile device updates the old time stamp $T_{S_{new}}$ TS with the new timestamp . Similarly it updates the old password PL with new one $P_{L_{new}}$ for next authentication session.

Thus, two-party authentication is achieved which is depicted in Figure. 2.

c) Sending of alerts to care-takers

In case of emergency, the MU contacts the web server's alert script with E = h (SID||IDL||NL||PL||GPS). NL denotes the sensed value if abnormal. If it is found to be valid, the web server fetches data from the database using the provided credentials and then forwards this information to the mail exchanger and SMS gateway from which the alert messages are send to the caretakers.

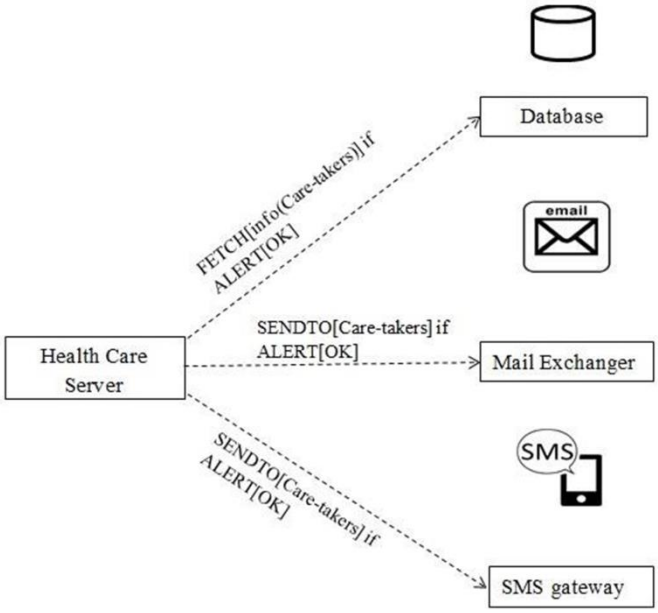

Figure 3. Alert Messages from Web Server

a) **FETCH** – Retrieve database details if authentication is successful.
b) **ALERT** – Intimate web server regarding user's emergency.
c) **SENDTO** – Sends the messages to the respective nodes.

This process is pictorially represented in Figure. 3. Once this communication is successfully completed, the webserver sends a message to the MU indicating successful communication.

Data Security in the Advanced Healthcare System

The data security is the most essential factor to be focussed in healthcare industries. For instance, if the temperature data of a patient is altered by the attackers, wrong treatment might be prescribed by the doctors which may even leads to death. In order to avoid this, data security requirements must be considered to accomplish data privacy and integrity.
ALE is a new Authenticated Lightweight Encryption algorithm. The basic operation of ALE is the AES round transformation and the AES-128 key schedule. ALE is an online single-pass authenticated encryption algorithm that supports optional associated data. Its security relies on using nonces. In a serial implementation, ALE has the distinct advantage over OCB3 by only requiring 4 AES round plus key scheduling per block, in contrast to full 10 AES rounds. ALE is actually significantly smaller than most other authentication encryption modes including the popular modes AES-OCB and AES-CCM. In terms of speed in the lightweight implementation, ALE is about 2.5 times faster than AES-OCB and about 5 times faster than AES-CCM [28]. The ALE algorithm allows the patient's history to be in encrypted form in the database instead of being stored in plain text, thus preserving the privacy of the data.

IV. ANALYSIS ON SECURITY, COMPLEXITY AND PERFORMANCE

Security Analysis

In this section, an analysis on security features is conducted to ensure that the proposed smart healthcare system is immune against possible attacks and also satisfies all the security requirements which are essential to offer secure communication in IoT based healthcare system.

Statement 1: The proposed protocol achieves secure mutual authentication

Proof: Mutual authentication in the proposed systems is a strong requirement that must be met to ensure secure communication between MU and the server. The smart devices and the server should pass each other's verification to legally verify each other. In the proposed protocol, the smart device and the server achieves the mutual authentication through two message exchanges: MA1 and MA2. Only the legitimate user can form a valid request message. After receiving the request message MA1 from a legal user, the server S verifies the time stamp TS received as part of MA1 with the one stored in the database. If those match, the server authenticates the MU. If the TS from MU does not matches with the one stored in the database, the access is denied. On the other hand, after receiving authentication request message MA2 from the server, the MU computes $R^* = h(SID || T_{S_{new}})$ from the known parameter SID and the derived parameter $T_{S_{new}} = DL \oplus SID$ from MA2 and checks whether the computed R^* matches with the received RS or not. If there is a match, the MU also authenticates the server. In this way, the proposed system satisfies the two-way authentication. Mutual authentication of users and service providers protects users from phishing as well as from insider attacks.

Statement 2: The proposed scheme protects user anonymity and untraceability property

Proof: Anonymity is the property of making the user untraceable from the attackers. The intruders must not be able to guess who sends the information. The proposed scheme could resolve this problem since the authentication request message MA1: {DL, AIDL, LM, RL, TS} does not contain any identity IDL of the user. Since the user's identity IDL is never sent in plaintext to the server S, neither the server S nor an intermediate attacker can determine the user's real

identity IDL. Moreover the authentication request message MA1: {DL, AIDL, LM, RL, TS} is based on random number and timestamp for current session. In addition to that $T_{S_{new}}$ generated by the server is different for each session as the server selects $T_{S_{new}}$ randomly for each session.

The different $T_{S_{new}}$ for different session reduces the possibility of linkability and avoids untraceability attack. The unlinkability and dynamic password usage concept ensures user anonymity and untraceability in the proposed scheme. In addition to this, the patient's details stored in the healthcare server and the data transmitted during communication is in encrypted form, so that the adversary can never discern who the patient is, which enables confidentiality. Padding of bits is also done which prevents the hash code to be monitored by the attackers. It confuses the intruder who tries to view the patient's details for malicious purpose.

Statement 3: The proposed scheme accomplishes Data Security

Proof: The protection of data security and entity privacy is the most important aspects for IoT- based healthcare systems. Data security is a privacy measure that prevents the data from unauthorized access. As the communication takes place via air medium, the data sent though it can be easily modified by the intruders, resulting in serious system damage to the entire system. So that the data should be secured by some means that the attackers could never guess it. In this proposed system, ALE algorithm is used to encrypt the data stored in the healthcare server. ALE is an online single-pass authenticated encryption algorithm that supports optional associated data. Its security relies on using nonces. This proves that this system offers more security.

Statement 4: The proposed scheme achieves Secure Localization property

Proof: Secure Localization is an important mechanism for tracking the exact position of the device. The patient's location estimation is needed for the success of the healthcare application. But this information must not be able to be traced by the attackers. The proposed lightweight algorithm can easily resolve this issue by XORing the location of the mobile unit LM with DL i.e) LM = GPS $\oplus$ DL which represents the physical connection between the MU and the healthcare sever. Subsequently, the server will retrieve the location of the mobile unit from the base station and verifies it with the one retrieved from LM. If the verification is successful, the server believes the legitimacy of the base station.

Statement 5: The proposed protocol achieves data integrity

Proof: The term data integrity refers to the act of verifying the correctness and consistency of data over its entire life-cycle. Data integrity ensures that a message that has been generated by a valid user and server has not been tampered with by an adversary. Hashing is a one-way function that offers data integrity. A cryptographic one-way hash function takes a variable length string as input, and generates a fixed-length n-bits string. The fundamental property of one- way hash function is that its output is very sensitive to even a slight change in input. The hash functions produce hash values of 128 bits and higher. In the proposed system, a key agreement is made using SHA-256 hash function to ensure data integrity. It produces a hash value of 256 bits. Since hash based message authentication is employed, the proposed method offers high data integrity. Thus the data transmitted in the network cannot be tampered, replayed and delayed maliciously.

Statement 6: The proposed scheme forbids replay attack

Proof: In replay attack, an attacker tries to send the previously captured messages i.e.) an adversary cheat the protocol entities by replaying previous used messages. An easy way to avoid this attack is using timestamps and random nonce. In the proposed protocol, the timestamp TS and a random nonce is sent along with the authentication request during transmission which provides additional security. Thus the protocol always rejects the attacker's trapped message MA1 due to the TS verification by the server. Moreover, an attacker cannot construct a new valid message, since the protocol uses the fresh nonce in each authentication request which helps to identify the duplicate messages. On the other hand, the adversary cannot replay the message MA2:{SID,RS, X}, since it cannot compute the updated timestamp $T_{S_{new}}$ in each session of authentication phase of the proposed protocol. Thus, the proposed protocol that includes timestamps and random nonce in the messages exchanged during authentication process will resist the replay attacks from both sides.

Statement 7: The proposed protocol is secure against man-in-the-middle attack

Proof: Man-in-the-middle attack can happen when an intruder sends a request to the server using a legitimate identity IDL to receive TS as an authentication token from the server during registration phase. After receiving the token TS, the intruder waits until the legitimate user U sends a request to the server. Once the genuine user sends a request to the server, an intruder intercepts the request and sends the stored token to the legitimate user. Now the user thinks that the TS is received from the valid server, so it sends response back to the intruder and then the intruder sends response to the server in response to the token sent initially. As the result of this, the network is tricked to authenticate the intruder. This problem can be mitigated by the proposed protocol as it provides strong and secure authentication. Assume that the attacker intercepts the transmitted message MA1:{DL,AIDL,LM,RL,TS} during the authentication phase. The attacker can only pass the authentication if he/she successfully computes AIDL= h (IDL||PL||R1||TS). The probability of successfully guessing IDL and PL is very low. As a consequence, the attacker cannot alter all the transmitted messages. Therefore, the proposed protocol could withstand the man-in-the-middle attack.

Statement 8: The proposed protocol is secure against impersonation attack

Proof: In impersonation attack, the attacker can eavesdrop all the transmitted messages over a public channel during protocol execution and can modify the eavesdropped messages and retransmit them to the user in order to impersonate as a valid user. The proposed scheme successfully defends impersonation attack in the following scenarios:

Suppose the attacker eavesdrops the message MA1:{DL,AIDL,LM,RL,TS} and tries to generate another valid message, which will be authenticated by the server. For generating the forged message, the attacker has to compute valid parameters which include DL, AIDL, RL and TS. The attacker however cannot compute valid RL= DL $\oplus$ R1 and AIDL= h (IDL||PL||R1||TS) as R1 and TS are unknown to him. Moreover, it is infeasible to guess all the unknown constraints simultaneously in polynomial time. Therefore, it is not feasible that the attacker can create or guess other valid messages in polynomial time. Therefore, the protocol provides strong security protection against the user impersonation attack.

On the other hand, our scheme is also secure against server impersonation attack. An attacker may try to impersonate the server by generating MA2:{SID,RS,

X}. However, the attacker cannot generate a valid RS= h (SID||$T_{S_{new}}$) without the knowledge of SID = DL $\oplus T_{S_{new}}$. Also, the attacker cannot generate a valid $T_{S_{new}}$. The attacker cannot extract the secret values due to the non-invertible one-way hash function property. As a result, it is proved that the proposed scheme is free from the server impersonation attack.

Statement 9: The proposed scheme achieves session key secrecy

Proof: The session key attack is a serious threat to all session key establishing scheme. Session hijacking is the process of utilizing of a legal session to gain illegal access to the information in a computer system. In the proposed scheme, the session ID, SID = DL $\oplus T_{S_{new}}$ is computed by the server.

- Since SID is hashed with one-way hash function, no information can be drawn from the session. Only partial hash code remains in the server and the other half is sent to the MU. Thus, even if one half of the session ID is compromised, it never helps the attacker to compromise the entire session.

- Each SID involves the usage of timestamp for computation where timestamps are unique for each session. Uniqueness property for different sessions guarantees unique SID for each session. This unique SID construction for each session ensures the freshness of SID. Usage of fresh $T_{S_{new}}$ at each communication session makes a session unlinkable from other session.

As the construction of a SID depends upon DL = h (IDL||PL) and randomly generated $T_{S_{new}}$, the attacker cannot compute it. Hence, our protocol is immune to session key guessing attacks.

Statement 10: The proposed protocol defends the eavesdropping attack

Proof: The parameters used during transmission of messages between MU and the server are hashed using one-way hash function which prevents eavesdropping attack. In this type of attack, the adversary can eavesdrop and record all the transmission between MU and the server during the authentication phase. During the execution authentication phase of the proposed protocol, the attacker can eavesdrops the transmitted message MA1 and collect the parameters DL,AIDL,LM, RL, and TS. Notice that AIDL is computed locally at MU as AIDL= h (IDL||PL||R1||TS) where R1 is a randomly chosen nonce of MU and it is unknown to the attacker. The parameter DL can be defined as DL = h (IDL||PL) and RL can be defined as RL= DL $\oplus$ R1 . If the attacker intercepts these parameters from the authentication request messages during transmission over the insecure channel, he cannot extract IDL, PL, and AIDL due to the hardness of one- way function. On the other hand, the attacker can eavesdrops the transmitted message
MA2 and collect the parameters SID,RS, and X in which RS can be defined as RS= h (SID||$T_{S_{new}}$) which requires hash operation for computation. Thus, the one-wayness of h(•) prevents the attacker from reaching any information from both MU and server . This proves that the system is resilient against eavesdropping attack.

Statement 11: The proposed scheme resists stolen smart device attack

Proof: An attacker can read the parameters {DL,AIDL,LM,RL,TS} of smart device, if it is stolen. Then, the attacker tries to generate a fake authentication request message. However, to generate a valid authentication request message MA1, user's identity IDL and Password PL are needed. Also, the attacker must guess the unknown parameters IDL and

PL at a time which is very difficult to do in polynomial time. The identity and password is neither stored in device nor attached to any message. The attacker may also try to guess the user's identity IDL or password

PL by monitoring the network message parameters {DL,AIDL,LM,RL,TS}. However, it is not possible to do so because all these parameters are protected by using h(•), which is a non- invertible one way hash function. Because of the collision-resistant one way hash function h(•), the attacker cannot guess any of the sensitive parameters. Therefore, it is then clear that our scheme protects this attack.

Complexity Analysis

The proposed scheme significantly reduces the communication and computation complexities. Most of past the solutions have unacceptable computation and communication costs. In contrast to existing protocols, the proposed lightweight protocol incurs lower communication and computation complexity. In this section, the computation and communication cost of the proposed protocol is analysed and compared with the existing system.

Computation overhead

Lightweight computation modules, such as one-way hash functions and bitwise exclusive-or operation, which are less computational complex, are exploited in the design of secure transmission for each protocol run. Table 4 demonstrates the computation complexity of the proposed scheme by comparing with the existing system.

Table 4. Comparative Analysis on Computation Complexities.

Steps	Number of Computations		
	BSN Care [20]	Proposed Scheme	Difference
Registration	2 Hash + 1 XOR + 3 CON	1 Hash + 0 XOR + 2 CON	-1 Hash, -1 XOR, -1 CON
Authentication	11 Hash + 8 XOR + 23 CON	8 Hash + 8 XOR + 12 CON	-3 Hash, -0 XOR, -11 CON
Total Computation Cost	13 Hash + 9 XOR + 26 CON	9 Hash + 8 XOR + 15 CON	-4 Hash, -1 XOR, -12 CON

*CON denotes a Concatenation operation

Since the number of hash function, $\oplus$ and || operations involved in computation of the protocol is minimized, the computation becomes simpler. The number of hash functions in the proposed algorithm is 9 and in BSN-care, it is 13. In the same way, the number of $\oplus$ operation and || operation in the existing system is 9 and 26 respectively whereas it is only 8 and 15 in the proposed system. This shows that the proposed scheme outperforms the existing system.

Communication overhead

The communication overhead is reduced by simplifying the decision making process. The mobile unit is responsible for processing the information and making decisions. Not all the information is sent to the server. Only during the emergency situation, the mobile unit activates the web server's alert script, thereby reducing the message traffic. The communication cost is analysed as follows and is compared with the existing healthcare system which is shown in Table 5.

Table 5. Comparative Analysis on Communication cost during authentication.

Protocol	**Number of communication**	**Communication structure**	**Total communication cost (in bits)**
Wu et al. [29]	3	U GW SN U	2048
Amin et.al [19]	4	U GW SN GW U	2112
Proposed	2	MU Server	1688

*U denotes User
*GW denotes Gateway
*SN denotes Sensor Node

The user and the server in the proposed protocol send messages MA1:{DL,AIDL,LM,RL,TS} and MA2:{SID,RS, X} respectively to the other party. The cost is measured in terms of bits length. The hash digest is 256 bits (since SHA-256 hash function is used), timestamp Ts, random nonce are 24 bits and GPS is 80 bits. So the communication cost from MU to server is 256+256+256+256+24=1048 bits and the communication cost from server to MU is 128+256+256= 640 bits. Therefore, the total communication cost of the proposed protocol is 1688 bits which is much lower than the existing protocols.

Performance Evaluation And Result Analysis

The performance of the proposed scheme is evaluated by practical implementation. The lightweight anonymous authentication protocol is implemented in order to analyse the performance, especially on security front and is compared with the existing protocol to manifest the advantages of the proposed scheme. The comparison is shown in Table 6.

Table 6. Comparison based on Security properties.

Security Requirements	Wood A et.al [6]	Ko. J et.al [11]	Li et.al [23]	Amin et.al [19]	Gope et.al [20]	Proposed Scheme
Data Integrity			✗	✗		
Anonymity	✗	✗				
Secure Localization	✗	✗	✗	✗		
Data Freshness		✗				
Data Security	✗	✗	✗	✗		
Mutual Authentication	✗	✗				

Table 7. Comparison based on Attack Resistance.

Attacks	Wood et.al [6]	Li et.al [23]	Amin et.al [19]	Gope et.al [20]	Proposed Scheme
Resistant to replay attack	✗				
Resistant to man-in-the-middle attack	✗	✗	✗		
Resistant to impersonation attack					
Resistant to session key attack				✗	
Resistant		✗			

to eavesdropping attack					
Resistant to stolen smart device attack	✗	✗	□	□	□

✓ means satisfied
✗ means not satisfied

From Table 7, it is clear that the proposed scheme can withstand several security attacks when compared to the protocols presented in [6], [23],[19] and [20] which are vulnerable to various security attacks.

From the above comparative analysis, it is concluded that the proposed protocol provides various types of security features with less communication and computation overhead. The experimental result shows that the overall processing time for the proposed system is about 4.37 seconds. This reduction in processing delay is directly associated with the improvement in automated healthcare system.

The experimental outcome indicates that the overall processing time for the proposed system is about 4.37 seconds. This reduction in processing delay leads to the improvement in automated healthcare system. The response time of telemonitoring system [10] is 8 min which is 99.09% higher than the proposed one. This reduction in response time of the proposed system is directly associated with the improvement of the system. The comparison detail is shown in Table 8.

Table 8. Comparison Based On Response Time.

Response Time	Telemonitoring system	Proposed System
	8 minutes	4.37 seconds

V. SIMULATION RESULTS

The Android application was developed on a smart phone of Oppo A33f with Quad-core processor as a test bed. The smart phone runs Android 5.1.1 operating system. In Figure.4, the screen shot shows that a BP of 180/100 and temperature of 107.1F is reported. The mobile device knows that this value is critical. This knowledge has to be given to the application beforehand. Once it is found to be critical it fetches the patient's detail from the server. After fetching the patient's detail, it reports the care takers and doctors with a critical message through SMS gateway and mail exchanger. In Figure.5, the screen shot shows that a BP of 120/80 and temperature of 98.5 F is reported. Therefore, no action takes place.

Figure 4. Health status indicating Critical

Figure 5. Health status indicating Good

VI. CONCLUSION

The proposed method aimed at facilitating healthcare at home to dependents using an automated system. At first, the WBSN design is simulated. Subsequently, a lightweight anonymous authentication protocol is proposed which is based on low-cost cryptographic primitives such as one-way hash function and Exclusive- OR operations. The proposed scheme also offers high data security by accomplishing all the security requirements of IoT based healthcare system. Moreover, the security analysis proved that the proposed protocol is robust against the possible security attacks. Most of the existing mechanism fails to reduce the communication and computational overheads. To overcome the weakness of the previous work, a reasonable mechanism is introduced to provide decision making capability to the device. In this method, only the critical messages are sent to the server instead of sending all the data. This automatic decision support mechanism for healthcare monitoring proves to be stable in terms of privacy and security and reduces the communication overhead. In addition to that, the number of hash function, $\oplus$ and $||$ operations involved in computations is minimized, therefore, the computation overhead is reduced. The reduction in communication cost is accomplished by means of reducing the total number of bits involved in communication. The comparative analysis proved that the proposed protocol is more cost effective and robust than the existing protocols. The Global Positioning System (GPS) allows detecting the location of the chronic patient at any place, at any time. The overall processing time is also reduced in the proposed scheme which brings improvement in smart healthcare system.

VII. REFERENCES

[1]. The evolution of internet of thing, TEXAS INSTRUMENTS, September 2013.

[2]. http://www.who.int/ageing/publications/global_health.pdf

[3]. Kumar P, Lee HJ, "Security issues in healthcare applications using wireless medical sensor networks: A survey," Sensors, Vol. 12, No. 1, pp. 55-91, Dec 2011.

[4]. Katagi, M. and Moriai, S.," Lightweight cryptography for the internet of things," Sony Corporation, pp.7-10, 2008.

[5]. http://automationrhapsody.com/md5-sha-1-sha-256-sha-512-speed-performance/

[6]. Wood A, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z.He, S. Lin, J. Stankovic, "ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring," Department of Computer Science, University of Virginia; Charlottesville, VA, USA:2006. Technical Report CS-2006-01.

[7]. Begonya Otal, Luis Alonso, Christos Verikoukis, "Highly Reliable Energy-Saving MAC for Wireless Body Sensor Networks in Healthcare Systems," IEEE Journal on Selected Areas in Communications, Vol. 27, No. 4, pp.553-565, May 2009.

[8]. Huang Y.M, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, "Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks," IEEE Journal on Selected Areas in Communications, Vol. 27, No. 4, pp.400- 411,May 2009.

[9]. Yanmin Zhu, Sye Loong Keoh, Morris Sloman, and Emil C. Lupu, "A Lightweight Policy System for Body Sensor Networks," IEEE Transactions on Network and Service Management, Vol. 6, No. 3, pp.137-148, September 2009.

[10]. Juan M. Corchado, Javier Bajo, Dante I. Tapia, and Ajith Abraham, "Using Heterogeneous Wireless Sensor Networks in a Telemonitoring System for Healthcare," IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No. 2, pp.234-240, March 2010.

[11]. Ko.J, J. H. Lim, Y. Chen, R. Musaloiu-E, A. Terzis, G. M. Masson, "MEDiSN: Medical Emergency Detection in Sensor Networks," ACM Trans. Embed. Comput. Syst. Vol. 10, No. 1, pp. 1–29, 2010.

[12]. Shyr-Kuen Chen, Tsair Kao, Chia-Tai Chan, Chih-Ning Huang, Chih-Yen Chiang, Chin-Yu Lai, Tse-Hua Tung, and Pi-Chung Wang "A Reliable Transmission Protocol for ZigBee-Based Wireless Patient Monitoring", IEEE Transactions on Information Technology in Biomedicine, Vol. 16, No. 1, pp.6-16, January 2012.

[13]. Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos, and Hua Fang, "ECG-Cryptography and Authentication in Body Area Networks," IEEE Transactions on Information Technology in Biomedicine, Vol. 16, No. 6, pp.1070-1078, November 2012.

[14]. Hu C, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body Area network security: A fuzzy attribute-based signcryption scheme," IEEE J. Select. Areas Commun. (JSAC), Vol. 31, No. 9, pp. 37–46, 2013.

[15]. Gope P, T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," IEEE Sensors Journal, Vol. 15, No. 9, pp. 5340 – 5348, 2015.

[16]. Yu S, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., Vol. 22, No. 4, pp. 673–686, 2011.

[17]. Xinghua Li,Hai Liu,Fushan Wei,Weidong Yang,"A Lightweight Anonymous Authentication Protocol Using k-pseudonym Set in Wireless Networks," IEEE Global Communications Conference (GLOBECOM), pp. 1-6, December 2015.

[18]. Chunhua Jin, Chunxiang Xu, Xiaojun Zhang, Jining Zhao,"A Secure RFID Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptosystem," Journal of Medical Systems, Vol. 39, No. 3, pp.1-8, March 2015.

[19]. Amin, Ruhul, SK Hafizul Islam, G. P. Biswas, Muhammad Khurram Khan, and Neeraj Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," Future Generation Computer Systems, 2016.

[20]. Gope P, T. 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.

[21]. Yeh, Kuo-Hui, "A Secure IoT-based Healthcare System with Body Sensor Networks," IEEE Access, 2016.

[22]. Gope P, T. Hwang, "Lightweight and energy-efficient mutual authentication and key

agreement scheme with user anonymity for secure communication in global mobility network," IEEE Systems Journal, Vol. 10, No. 4, pp.1370-1379, Dec 2016.

[23]. Li, X., Peng, J., Kumari, S., Wu, F., Karuppiah, M. and Choo, K.K.R., "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," Computers & Electrical Engineering, 2017.

[24]. Deebak, Bakkiam David, Fadi Al-Turjman, Moayad Aloqaily, and Omar Alfandi, "An authentic- based privacy preservation protocol for smart e-healthcare systems in IoT," IEEE Access 7, pp.135632-135649, 2019.

[25]. Li, Xiong, Jieyao Peng, Mohammad S. Obaidat, Fan Wu, Muhammad Khurram Khan, and Chaoyang Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," IEEE Systems Journal 14, no. 1, pp.39-50, 2019.

[26]. Zhang, Yinghui, Dong Zheng, and Robert H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," IEEE Internet of Things Journal 5.3, pp. 2130-2145, 2018.

[27]. Wang, Guoming, Rongxing Lu, and Yong Liang Guan. "Enabling efficient and privacy-preserving health query over outsourced cloud." IEEE Access 6, pp. 70831-70842,2018.

[28]. Bogdanov A, Mendel F, Regazzoni F, Rijmen V, Tischhauser E., "ALE: AES-based lightweight authenticated encryption," Springer, Vol. 8424, pp. 447-466, 2014.

[29]. Wu, F., Xu, L., Kumari S. and Li, X., "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks," Multimedia Systems, pp.1-11, 2015.

Authors

P.Jeyadurga is working as Assistant Professor in the department of Computer Science and Engineering at Dr.Sivanthi Aditanar College of Engineering, Tiruchendur. She completed her Bachelor Degree in Computer Science and Engineering at VV College of Engineering, Tisaiyanvilai in 2015 and her M.E Computer Science and Engineering in VV College of Engineering, Tisaiyanvilai in 2017. Her areas of interest include Internet of things and Network Security.

S.Ebenezer Juliet is working as Associate Professor in the department of Computer Science and Engineering at V V College of Engineering, Tisaiyanvilai. She completed her Bachelor Degree in Computer Science and Engineering in Government College of Engineering, Tirunelveli in 1995 and her M.E Computer Science and Engineering in Manonmaniam Sundaranar University in 2004. She completed her Doctoral degree in the area of Compound image compression. Her
areas of interest include Image Compression and Computer Graphics.