Multi-Factor Remote User Authentication Scheme for WSN-IoT based Healthcare Services

Rajinder Vir[1], Vikrant Sharma[2]
LKCTC, Jalandhar, Punjab[1]
GNA University, Phagwara[2]
Corresponding author: Rajinder Vir, Email: rajindervir@lkcengg.edu.in

With the growth of Wireless Sensor Networks and Internet of Things (IoT) paradigms, real-time remote monitoring of the patients by a remote Medical Professional (MP) has become feasible and patients can enjoy healthcare services at home. However, patient's medical data stored on servers are highly sensitive and hence, the Wireless Sensor Networks-IOT network becomes open to many attacks. Therefore, it must ensure that patients' medical data do not get exposed to unauthorized users. This makes strong user authentication essential for the successful global deployment of centralized healthcare systems. In this paper, we present an efficient, strong authentication protocol, for the MP to access patient data for healthcare applications based on Wireless Sensor Networks-IOT network. The proposed protocol includes (1) three-factor MP authentication (i.e., password, biometrics, and smartcard); (2) mutual authentication between MP and the Wireless Sensor Networks server; (3) establishing a secure shared session key; and (4) maintaining key freshness. Furthermore, the proposed protocol uses only two message exchanges between MP and Wireless Sensor Network server and attains efficiency (i.e., low computation and communication costs). Through the formal analysis using the AVISPA web tool, security analysis, and performance analysis, we conclude that the proposed protocol is more secure against potential attacks, and obtains a trade-off between security and performance costs for healthcare applications using Wireless Sensor Networks-IOT networks.

Keywords: Authentication, Biometrics, Big data, WSN; ECC, Healthcare, IoT.

2023. In Vikram Dhiman & Pooja Dhand (eds.), *Emerging Trends in Engineering and Management*, 151–172. Computing & Intelligent Systems, SCRS, India.
https://doi.org/10.56155/978-81-955020-3-5-17

1 Introduction

Internet of Things (IoT) and next-level big data analytics tools are promising Information Communication Technology (ICT) paradigms possessing potential to transform healthcare services. This is due to the increased pervasive existence of smart devices embedded with Radio Frequency IDentification (RFID) tags, sensors, and actuators nodes, having unique IP addresses. By using the unique address, these objects can communicate together and use data gathered, for producing interpretations or predicting some results [1]. Big data analytics tools can aid the physicians use complex predictive analysis for early prediction of certain diseases from the patient's Electronic Health Records (EMRs). This will allow prevention of chronic ailments, reduce treatment costs, personalized and better healthcare facilities. Also, physicians can use big data analytics tools for checking out alternative treatment options for a particular patient based on factors such as, personal history, prior health issues, and hereditary data.

Furthermore, the innovative advancements in Wireless Body Area Networks (WBANs), has allowed several wearable sensors and devices deployed on to patient body. This allows for ubiquitous monitoring and tracking of physiological data and health related information. Integrating WBANs with IoT, Wireless Sensor Networks and big data technologies will allow for real-time monitoring of patients anytime, and anywhere. This led to the development of Real-time Health Systems (RTHS). These systems will be vital for healthcare in IoT, because Big Data Analytics tools and processes will be applied to estimate both dynamic and static data for predictive analysis. Since these systems will operate in heterogeneous wireless environments which are insecure, they require secure communication of patient's health information along with a guarantee of data integrity and confidentiality for reliable healthcare architecture. Major challenges of RTHS are i) key management for secure communication ii) secure data forwarding and iii) Patient-centric access control to the stored EMRs.

In this paper, we have proposed a new lightweight key management and authentication protocol for healthcare services based on Wireless Sensor Networks-IOT and big data environment. The protocol establishes a secure communication channel between a physician and a remote entity (i.e. Wireless Sensor Networksserver). Using this secured channel physician can access patients EMRs stored on Wireless Sensor Networksserver while ensuring confidentiality and authentication. Our protocol considers a network model consisting of a centralized healthcare authority to which several hospitals are connected. The network model is shown in Figure 1.

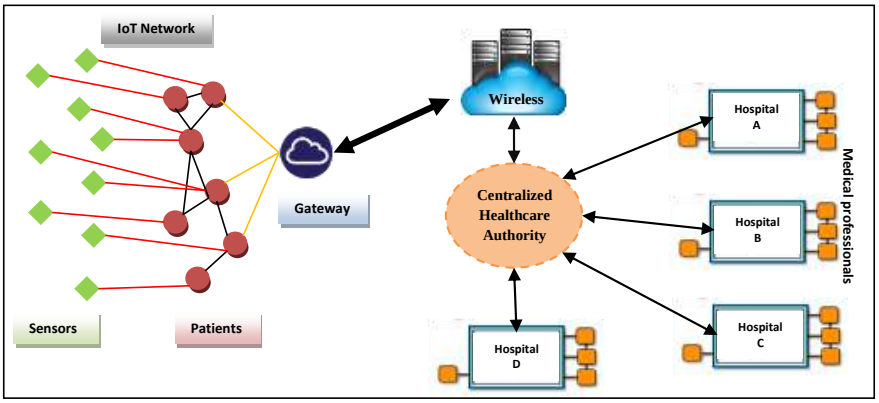

Figure 1. WSN-IoT healthcare service architecture

1.1 Motivations

Authentication and key establishment play a significant role in heterogeneous environments and this has led to the development of several schemes for providing secure communication. These schemes have their own advantages and disadvantages. To best of our knowledge, there is no proposed key establishment and authentication scheme specific for a centralized Wireless Sensor Networks-IOT and big data based healthcare applications until now. In fact, in a centralized Wireless Sensor Networks-IOT environment, we need a key establishment scheme, which allows a physician or medical professional to securely access EHRs from the Wireless Sensor Networksserver. This can be provided using a multi-factor authentication scheme. The aim of this paper is to present a key establishment scheme and authentication scheme for RTHS, which satisfies essential security and efficiency requirements and maintains low communication and computation overhead.

1.2 Our contributions

- We present a scenario for Wireless Sensor Networks-IOT based Healthcare system along with various threats and security model.
- We propose a secure authentication protocol based on ECC for remote patient monitoring in Wireless Sensor Networks-IOT environments. The protocol is a multi-factor protocol because it uses three different factors for preserving user identity: password, smart card and biometrics. The use of biometrics increases the security of the protocol because biometrics is difficult to forge or steal or forget.
- We prove our scheme secure using a formal proof and analysis.
- We simulate our scheme using AVISPA tool for the formal security analysis and demonstrate that the proposed scheme is secure against active and passive attacks.
- We perform a comparative evaluation of our scheme with some latest schemes in terms of communication and computational overheads.

1.3 Paper organization

The rest of the paper is organized as follows: *Section 2* discusses the work related to user authentication in healthcare applications. Next, we demonstrate the proposed remote health-monitoring system, threat model and different security requirements in *Section 3*. We then discuss some preliminaries of ECC, one way hash functions in *Section 4*. The proposed authentication protocol is discussed in *Section 5*. *Section 6* discusses the security and performance analysis of the proposed protocol. *Section 7* gives a detailed formal verification of the proposed protocol using AVISPA. *Section 8* presents the comparison of the protocol with other related schemes proposed in literature. Finally, *Section 9* concludes.

2 Related Work

Wireless Sensor Networks and IoT promises an innovative paradigm shift which will allow interconnecting several sensors, smart devices to gather and share data for observation and interpretation. This evolving merger offers a wide range of potential applications that can improve the quality of people's life. The most promising and upcoming potential application is real time remote patient healthcare monitoring and tracking, where a remote patient's health related data gets accumulated with the help sensors, which is then delivered through internet and can be accessed by healthcare professionals for analysis and evaluation of patient's health. In this section, we discuss the existing studies carried out by researchers for providing authentication in remote patient healthcare monitoring and extract out the limitations of the existing work.

In 2004, *Watro et al.* [2] developed a public-key-based protocol for authentication. The protocol allowed exchange of data between a sensor network and a third party as well as between two sensor networks.

In 2005, *Benenson et al.* [3] developed a user authentication protocol based on elliptic curves which is robust to several attacks and handles the sensor node capture attack properly. However, the protocol fails to offer mutual authentication, data confidentiality, integrity, and is also vulnerable to DoS attacks, node compromise attacks.

In 2006, *Wong et al.* [4] proposed a user authentication protocol for WSNs. The protocol is lightweight and is composed of registration, login and authentication phases. It provides security from replay and impersonation attacks however it does not provides mutual authentication, data confidentiality, secrecy and scalability and doesn't provide resistance against attacks such as stolen verifier attacks, sensor node compromise attacks, etc.

In 2007,*Tseng et al.* [5] developed a user authentication protocol having password change phase on *Wong et al.'s* [4] protocol. Still the protocol fails against several potential attacks and threats and has no provide mutual authentication. *Hu et al.* [6] created a real-time healthcare monitoring system for cardiac patients. In their architecture patient's ECG signals gets collected automatically to a server from where the professional can access the data for further analysis and generating reports. The proposed architecture offers data confidentiality and integrity; however, strong user authentication is lacking.

In 2009, *Das* [7] gave an authentication protocol for healthcare based on wireless sensor networks. The protocol is defenceless against several attacks such as node bypass, user impersonation, and insider attack and also doesn't provide message confidentiality, and mutual authentication. *Huang et al.* [8] designed a secure architecture for sensor-based healthcare monitoring. Their hierarchical system however lacks strong user authentication, which is critical for remote healthcare services. *Malasri et al.* [9] presented an ECC based key agreement protocol for mote-based medical sensor network based healthcare services. In this protocol, two-tier architecture is employed to authenticate access to patient data. The scheme provides sufficient security to patient's data but it doesn't provide strong authentication for health professional that can access patient's data which can open to backdoor to attackers. *Sriram* [10] designed a security framework for securing remote health monitoring systems based on sensor networks. Their proposed architecture provides secure exchange of patient's data across the sensor network.

In 2010, *Sarier et al.* [11] proposed a multi-factor protocol for allowing secure communication between two entities and establishing key agreement with server. *Venkatasubramanian et al.* [12] presented a protocol for physiological signal-based key agreement for authenticated communication between neighbouring nodes in an MSN. A multi-factor user authentication protocol was proposed by *Yuan et al.* [13] for WSNs. The protocol was resistant to replay attacks, denial attacks, and forgery attack but was susceptible to insider attack, DoS attacks and impersonation attacks. Also it didn't provide mutual authentication, data integrity, password change and key agreement.

In 2011, *Chen et al.* [14] proposed an authentication protocol suitable for applications having strong security needs. *Le et al.* [15] proposed an access control protocol based on ECC that allowed mutually authenticated professionals to access patient's data. The protocol is defensive against replay and denial-of-service attacks. However it is vulnerable to leakage attacks and hence, can pose a serious risk to patient's privacy, therefore not suitable healthcare. *Yeh et al.* [16] found that *Chen et al.'s* [17] protocol did not allow the user to update password and was susceptible to insider attack and other attacks. They then proposed a new improved authentication protocol for WSNs based on elliptic curve cryptography (ECC). *Yoon et al.* [18] proposed an improved user authentication for WSNs. They also reviewed *Yuan et al.'s* [13] protocol and found that it did not provide data integrity. But their protocol also had no key agreement, and was susceptible to compromise attacks.

2.1 Attack model and security issues

Like any system, public Wireless Sensor Networks-IOT system must be secured against the common adversaries such as, spammers, hackers, malware, etc. An adversary refers to any malicious entity which intrudes the system with the aim to prevent the legitimate users from achieving their goals of privacy, integrity, and availability of data. He might attempt to access secret data, manipulate the data in the system, and spoof the identity of a legal sender or receiver, and many more. We presume that adversary can step in each and every communication paths, and is therefore capable of altering or copying messages, replaying them, or injecting false data or messages. This section will summarize the possible threats to the patient's data stored on Wireless Sensor Networksserver and critical security requirements.

2.1.1 Attack model

Wireless Sensor Networks-IOT based environments face the same set of threats similar to any conventional network. However, due to the huge amount of data that is being stored on the Wireless Sensor Networksservers, the Wireless Sensor Networksservice providers become an easy and attractive target for the attackers. These threats/attacks may originate from different entities with their adversary models.

a) *Eavesdropping*. This attack refers to illegal interception of a communication between two entities. Such attacks can occurs when the Wireless Sensor Networksservice provider accesses the data stored on the server out of curiosity. These attacks are menacing since they are difficult to identify and the users unknowingly storing sensitive data such as passwords, etc. on the server.
b) *Integrity attack*. A data integrity attack occurs when an attacker tries to corrupt or manipulate data without permissions of the owner. The attack is usually carried out via malware program that deletes or modifies contents of a smart device.
c) *Denial attack*. In this attack one of the communicating parties denies either all or some part of the transmission tasks.
d) *Denial of Service attack*. This attack happens when a Wireless Sensor Networksserver is flooded by large number of service requests which it cannot handle. It can cause the server to crash and legitimate users are denied from service.
e) *Wireless Sensor Networksserver compromise attack*. This attack occurs when an attacker gains control of the server after network deployment. An attacker can connect to a server and can completely control it for fetching the information or controlling that server and its further communication.
f) *Replay attack*. This attack takes place when the malicious entity spies the ongoing communication that takes place between the two parties. The malicious entity collects the authenticated information, e.g., shared session key and then tries to contact the receiver later on with that key. The attacker simply replays the eavesdropped message.
g) *Impersonation attack*. In this attack the attacker is tries to impersonate a legal entity and tries to communicate with the other entity as a legitimate entity.

2.1.2 Security requirements

In order to augment the inherent security for remotely monitoring of patients for being suitable to various applications and services, we have identified several security requirements to be taken care of while building a secure authentication protocol. These requirements are defined as follows:

a) *Mutual authentication*. This requirement states that before the patients' data is accessed by a MP from the Wireless Sensor Networks server, authentication should occur between Wireless Sensor Networks server and the MP. The two-way authentication is a process in which the communicating parties authenticate simultaneously.
b) *Confidentiality*. This requirement states that the secret information must be transmitted in a secure manner over the communications. For that reason, the data from the sensors in an IoT

network e.g., health data collected from patients must be transmitted in an encrypted form onto the Wireless Sensor Networks so that only the recognized data consumers can recognize it. Also, when the data consumers try to fetch the patient's data stored on cloud, data is accessed in an encrypted manner.

c) *Anonymity*. This requirement states that the adversary must not be able trace any sensor data by using interactions with it. In case the exchanged sensor data doesn't satisfies anonymity, the attacker having same provider will easily track owner of a specific sensor or be able to discover the location of the data owner.

d) *Availability*. Authentication process must be executed every time whenever the data consumer tries to access sensitive information stored on the Wireless Sensor Networks about the data owner. Availability ensures that the data consumer must be able to access all the time from the Wireless Sensor Networks service provider.

e) *Forward security*. This requirement states that the information transmitted previously is untraceable using the currently transmitted information. If the previously exchanged messages are easy to be traced using the intercepted information, it can result in serious privacy risks.

f) *Scalability*. Scalability enables a system to handle growing amounts of work in a graceful manner. The Wireless Sensor Networks-IOT system must provide opportunity for the IoT networks to scale their computing resources whenever they deem it necessary. Hence, the computational workload must be sustained by the Wireless Sensor Networkswith the increase in the sensors in the IoT networks.

3 Preliminaries

3.1 Notations

The notations used in the scheme are listed below:

Table 1. Notations used

Symbol	Description
p	Large prime number
Z_n	Finite field
E	Elliptic curve
G	Generator point on elliptic curve E having order q
MP	Medical professional
CS	Wireless Sensor Networksserver
ID_{MP}	Identity of MP
PW	MP's password
B_{MP}	MP's biometric imprint
BIO_{MP}	Perceptually hashed biometric
$E_K(m)$	Encryption operation using K

$D_K(c)$	Decryption operation using K
$\oplus$	XOR operation
||	Concatenation operation
h(.)	Perceptual hash function
H(.)	One-way hash function
$T_1, T_2,$ T_{curr}	Timestamps
a, u, y_{MP}	Random number

3.2 Perceptual Hashing

When using biometrics for user authentication schemes, the standard encryption or hashing algorithms cannot be used to encrypt the biometric template. This is because biometric data, e.g., fingerprint, voice etc. changes with time and environment. To resolve this issue researchers have suggested using Perceptual Hashing (P-Hash) [54]. In this approach, a hash value is computed for a multimedia data and it remains more or less the same if the content is not modified significantly. The benefit of using P-Hash is that it can tolerate minor variation in quality and format of the input. The size of the hash value generated by perceptual hashing varies from 64 bits to 128 bits. The process of perceptual hashing is shown in Figure 2.

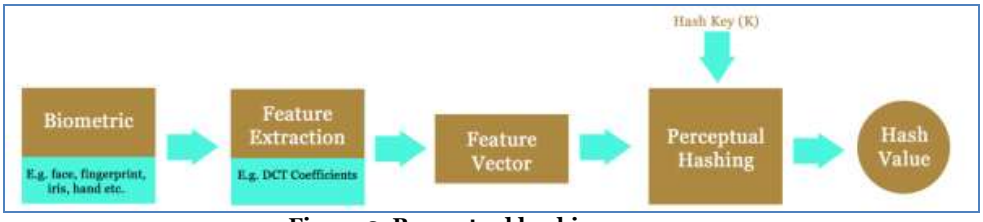

Figure 2. Perceptual hashing process

4 Proposed Protocol for Sensor Data

The proposed Wireless Sensor Networks-IOT based healthcare scenario of Figure 1 consists of seven entities particularly in the authentication protocol. These are patients, medical professionals, sensor nodes and Wireless Sensor Networks server.

a) **Patient** is a passive entity receiving a particular treatment and registered with the healthcare authority to receive medical supervision.

b) **Sensor nodes** are active entities and are small tiny sensors which are deployed onto patient's body for observing health related figures like BP, temperature, heart beat rate, etc.

c) **A wireless sensor network (WSN)** also referred as Wireless Sensor and Actuator Networks (WSAN), are active entities and consists of sensors which are spatially scattered and

independent and which continuously or on demand monitor and track the environment conditions and pass the observed data to Wireless Sensor Networks server.

d) **Patient Gateway** refers to a node providing access to another network using different protocols and allows transmitted data to use its routing paths.

e) **Medical Professional (MP)** can be either doctor, surgeons, nurses, etc. who can access patient's information through Wireless Sensor Networks-IOT framework.

f) **Healthcare Authority (HA)** is the primary entity which provides quality healthcare services, assures collecting, analysis and disseminating health related information to its registered patients through its registered set of MPs.

g) **Wireless Sensor Networks server** the main server playing the major role of storing the healthcare data of the patient, the MP can access the data by logging into the Wireless Sensor Networks server and once the server authenticates he/she can access it.

The authentication protocol proposed in this paper will allow the MPs to securely gain access to the patients' health data stored on the Wireless Sensor Networks server. The notations used in the paper are shown in Table 1. The proposed protocol is composed of four phases:

Phase 1: Patient registration phase,

Phase 2: MP registration phase,

Phase 3: Pre-computation and Login phase,

Phase 4: Authentication phase,

4.1 Phase 1. Patient Registration phase

The proposed protocol requires the patient to register at the healthcare authority which is the registration center at the hospital. To successfully register, patient sends a registration request message along with his name and medical diagnosis to the healthcare center. The healthcare authority selects the required sensor kit as per the diagnosis of patient's condition and allocates suitable MPs. The healthcare authority also generates a unique identity for the patient and supplies the medical kit along with the unique identity to the patient. A technician from the hospital then deploys the sensors onto the patient's body.

4.2 Phase 2. Medical professional registration phase

The MP who is the active user in the proposed protocol needs to get himself/herself registered with the Healthcare Authority (HA). The HA will generate a suitable security key information for the MP. The process is shown in Figure 3.

a) Over the secure channel the MP will submit his identity ID_{MP}, password PW_{MP} and biometric information B_{MP} to Wireless Sensor Networks server.

b) Next, the Wireless Sensor Networks server will compute perceptual hash of input biometric B_{MP} as $BIO_{MP}=h(B_{MP})$. It also generates a random numbery_{MP}. It then calculates

$T_{MP}=H(ID_{MP}||PW_{MP}||BIO_{MP})\oplus H(X)$ and $R_{MP} = H\ (ID_{MP}||PW_{MP}||BIO_{MP})\oplus H(y_{MP})$. Also, the Wireless Sensor Networksserver calculates $S_{MP}= y_{MP}\oplus ID_{MP}\oplus PW_{MP}\oplus BIO_{MP}$. It then through a secure channel sends <T_{MP}, R_{MP}, S_{MP}> to MP.

c) MP will receive a smart card with <T_{MP}, R_{MP}, S_{MP}> stored into it.

d) Next, the Wireless Sensor Networksserver computes $D_{MP} = H(H(ID_{MP}||y_{MP})\oplus X)$ and stores $D_{MP}, y_{MP}\oplus X, ID_{MP}\oplus H(X||y_{MP})$ into its memory.

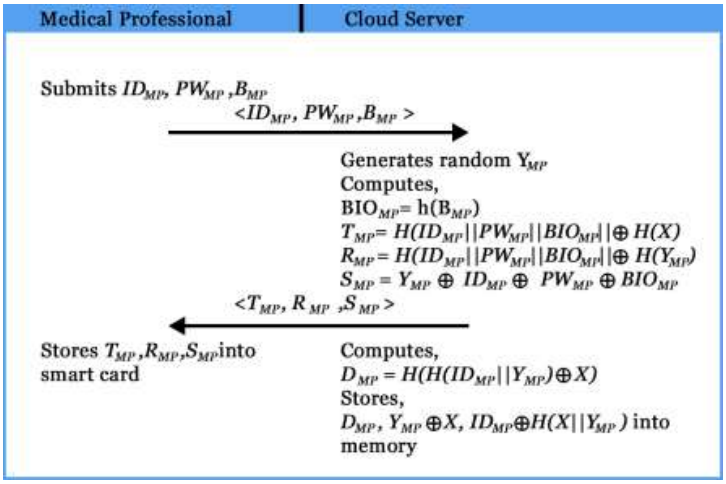

Figure 3. Registration phase for Medical professional

4.3 Phase 3. Pre-computation and Medical professional login phase

For accessing patient's healthcare data stored on Wireless Sensor Networksserver, MP, must login into the Wireless Sensor Networksserver and get authenticated first. The MP performs following steps to login:

a) The medical professional MP, uses smart card and submits the login credentials viz. identity, secret password and his/her personal biometric information, i.e., ID'_{MP}, PW'_{MP} and B'_{MP}. It then computes the perceptual hash of the entered biometric as $BIO'_{MP} = h(B'_{MP})$.

b) Next, the MP generates random number, **a** and calculates the ECC point A as $A = a \times G$ and $c = a \times P_{CS}$.

c) The MP then calculates $y'_{MP} = S_{MP}\oplus ID'_{MP}\oplus PW'_{MP}\oplus BIO'_{MP}$ and $R'_{MP} = H(ID'_{MP}\oplus PW'_{MP}\oplus BIO'_{MP})\oplus H(y'_{MP})$.

d) The MP then checks if $R_{MP}^{'} ?= R_{MP}$. If the condition holds, the information entered is correct and it continues further otherwise the login process gets terminated because some illegitimate user is trying to access the server.

e) Next, it computes $H(X) = S_{MP} \oplus H(ID_{MP}||PW_{MP}||BIO_{MP})$ and $MID = H(ID_{MP}||y_{MP} \oplus H(X)$ and also, $Z_{MP} = H(ID_{MP}||H(X)||y_{MP})$.

f) Next, it encrypts A using Z_{MP} i.e. $E_{Z_{MP}}(A)$ and also computes $\beta = H(Z_{MP}||T_1)$. It then forwards the login request $< MID, E_{Z_{MP}}(A), \beta, T_1 >$ message to the Wireless Sensor Networksserver.

The workflow of the steps is shown in Figure 4.

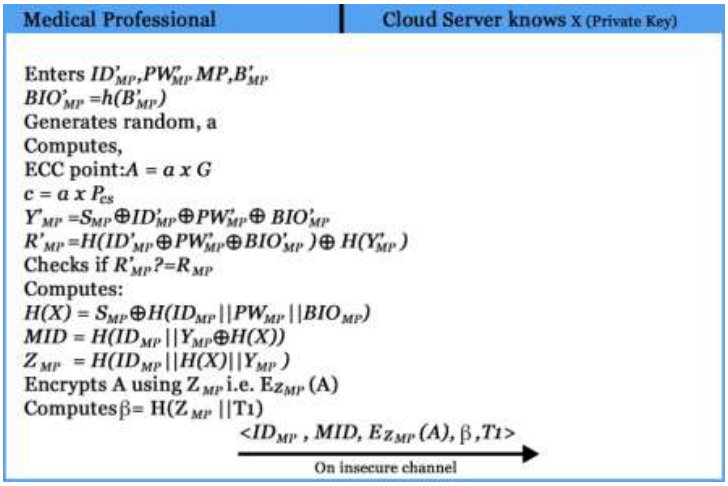

Figure 4. Login request by Medical professional to Wireless Sensor Networksserver

4.4 Phase 4. Authentication Phase

During this phase, the Wireless Sensor Networksserver authenticates the MP. This phase is required so that only a legitimate MP can get access to the sensitive patient data stored on the Wireless Sensor Networksserver. The steps of the process are:

a) The Wireless Sensor Networksserver will receive login request message and will check if $(T_1 - T_{curr}) \leq \Delta T$? If the check doesn't hold, the login process gets terminated. Otherwise, Wireless Sensor Networksserver computes $D_{MP}^{'} = H(MID \oplus H(X) \oplus X)$. This check allows handling the message replay attacks.

b) Next, it checks for the condition if $D_{MP}^{'} = D_{MP}$? If the condition fails, the server terminates the process, else the Wireless Sensor Networksserver calculates $Z_{MP}^{'} = H(ID_{MP}||H(X)||y_{MP})$ and $\beta' = H(Z_{MP}^{'}||T_1)$ to verify whether the message has been send by a legal MP.

c) Next, the Wireless Sensor Networksserver checks for the condition if $\beta' = \beta$? This check again allows taking care of the message replay attacks, since if the value of the timestamp got modified the condition will fail to hold and the Wireless Sensor Networksserver will cancel the login request by rejecting the login message. If not, the Wireless Sensor Networksserver will decrypt A using Z'_{MP}, i.e., $D_{Z'_{MP}}\left(E_{Z_{MP}}(A)\right)$ to extract A.

d) The Wireless Sensor Networksserver will compute $c = A \times X_{CS}$ and $L = H(A||T_2)$. It next, generates a random number u to compute $\gamma_{CS} = H(c||u||Z'_{MP}||T_2)$. It then transmits the message to the MP's smart device, i.e., $< \gamma_{CS}, u, L, T_2 >$ and computes session key i.e. $S_K = H(H(X)||Z_{MP}||c||u)$.

e) The MP will receive the message $< \gamma_{CS}, u, L, T_2 >$. The smart device will then check for the condition if $(T_2 - T_{curr}) \leq \Delta T$ satisfies or not. In case the condition doesn't satisfies, the request message is rejected, since it's a previously intercepted message replayed again by the illegitimate user. Otherwise, the smart device computes $L' = H(A||T_2)$.

f) Next, the smart device checks for the condition if $L' = L$? if the condition holds, the message is sent by a legitimate Wireless Sensor Networksserver otherwise the process terminates indicating that the message has been intercepted and modified during transit.

g) If successful, the smart device computes $\gamma'_{CS} = H(c||u||Z_{MP}||T_2)$ and checks if the condition holds or not, i.e., $\gamma'_{CS} = \gamma_{CS}$? If the condition fails, the message is rejected, otherwise, the device calculates shared session key as $S_K = H(H(X)||Z_{MP}||c||u)$.

Figure 5 shows the authentication process.

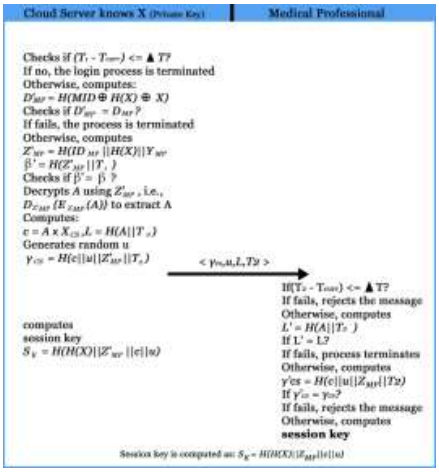

Figure 5. Authentication and key agreement phase

5 Performance and security analysis

This section discusses the informal protocol verification against the security and performance requirements specified in the *section 3*. Although achieving security of authentication protocols is extremely important however it is also difficult to accomplish. The proposed authentication scheme establishes a shared session key between the Wireless Sensor Networksserver and the MP also offers mutual authentication between them, and is defensive to all the attacks discussed in *section 3.1.1*.

5.1 Informal security analysis

5.1.1 Provides mutual authentication

The proposed protocol guarantees mutual authentication between the Wireless Sensor Networksserver and MP. In the proposed protocol, the MP before accessing sensitive IoT sensor node data about a patient mutually authenticates with the Wireless Sensor Networksserver so as to verify the authenticity of the server. The Wireless Sensor Networksserver authenticates the MP when the condition $D_{MP}^{'} = D_{MP}$ holds. Similarly the MP authenticates the Wireless Sensor Networksserver if $\gamma_{CS}^{'} = \gamma_{CS}$ and $L^{'} = L$ holds.

5.1.2 Provides confidentiality

The proposed protocol provides confidentiality by transmitting sensitive data in an encrypted form to the Wireless Sensor Networksserver. Transmitting sensitive data without encoding over insecure channel, will allow attacker easily observe the ongoing communication. The session key is generated independently by the Wireless Sensor Networksserver and MP. Message confidentiality protects against eavesdropping attacks.

5.1.3 Provides anonymity

The MP communicates with the Wireless Sensor Networksserver in network via open insecure wireless channel. The proposed protocol provides user anonymity by employing multi-factors i.e. biometric information B_{MP} as unique identification of the MP which is impossible to forge, along with the password PW_{MP} thereby securing disclosure of any private information even if any illegitimate user eavesdrop the communication.

5.1.4 Provides forward security

Ensuring forward security requires that even if legitimate user's secret key is leaked out it will not compromise the session key generated. In the proposed protocol, if the MP MP's key is compromised; any intruder is still unable to generate the session since, to generate the session key $S_K = H(H(X)||Z_{MP}||c||u)$, the adversary needs both ID_{MP} MP's identity, private key X, parameter c and u. Also, the adversary needs to resolve ECDLP which is a computationally hard problem and he cannot predict c and L. This proves that the proposed protocol provides forward secrecy.

5.1.5 Provides scalability

The proposed protocol provides scalability. This property allows the system to expand. Any number of patients can be added to the system without affecting the system. Since the Wireless Sensor Networksserver does not store or maintain any verifier table or any database of passwords. Hence, the proposed protocol offers scalability.

5.1.6 Efficient login phase

In proposed protocol, during MP login phase, the smart device of a legitimate medical processional verifies the correctness of inputs ID_{MP}, PW_{MP} and $B_{MP}^{'}$using the condition if $R_{MP}^{'}? = R_{MP}$. If the condition satisfies, the smart device executes the further else terminates the login process. This proves that the proposed protocol effectively finds the validity of data provided by the MP.

5.1.7 Known key secrecy

In proposed protocol, even if the session key $S_K = H(H(X)||Z_{MP}||c||u)$ of previous communications gets leaked to an attacker, he still cannot use it to predict the information of other session keys because each session key is generated using one-way hash functions. Hence, no intelligence gets extracted from the session key.

5.1.8 Key freshness

In the proposed protocol, each established session key $S_K = H(H(X)||Z_{MP}||c||u)$ includes a fresh random number u. The use of fresh random numbers allows achieving the freshness of the key for every communication session. This allows that an exclusive key is generated every time. Therefore, the exclusiveness ensures the key freshness.

5.1.9 Resistance to man-in-the-middle attacks

The proposed protocol protects against man-in-the-middle attack. This attack arises when an attacker is able intercept the communication between a legal MP and Wireless Sensor Networksserver and he/she able to successfully masquerade as legal user to other entities. In the proposed protocol, each of the entity (MP and Wireless Sensor Networksserver) mutually authenticates each other which let the proposed protocol to successfully prevent the attack.

6 Automatic formal verification using AVISPA

The developed protocol is simulated in AVISPA (Automated Validation of Internet Security Protocols and Applications) tool. It is a web based push button tool using which the formal security verification of the security protocols is carried out. To simulate the protocols the user codes the protocols in HLPSL (High Level Protocols Specification Language). AVISPA consists of a *translator tool* called HLPSL2IF and four back-ends. The *translator tool* is used to convert a protocol written in HLPSL into Intermediate Format (IF). This IF is a general language understood by all the back-ends and is used

by different back-ends to test and analyze different properties specified in the protocol. These back-ends are [55]:

- Constraint-Logic based Attack Searcher (CL-AtSe)
- Onthe-fly Model-Checker (OFMC)
- Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP).
- SAT-based Model-Checker (SATMC)

The structure of the AVISPA tool is shown in Figure 6.

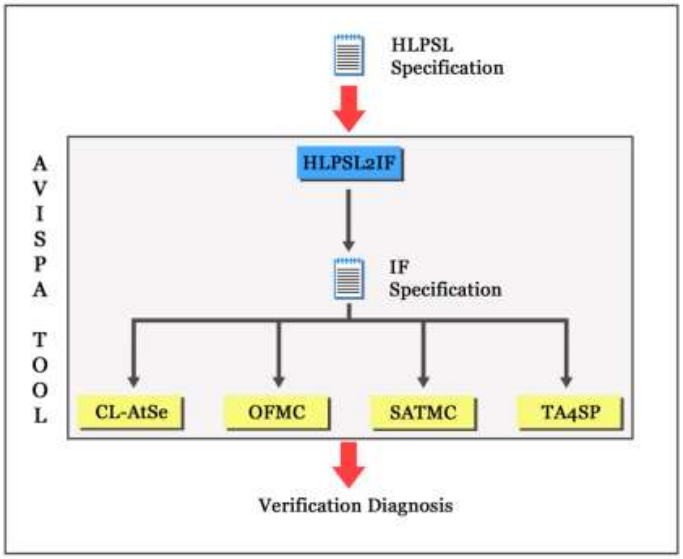

Figure 6. Structure of AVISPA [55]

These back-ends produce the Output Format (OF), having following parts:

- **SUMMARY**: This section tells whether the proposed protocol is safe, unsafe, or whether the analysis is also inconclusive.
- **DETAILS**: This section tells under what conditions the proposed protocol was concluded safe, or an attack is found, or why the result was inconclusive.
- **PROTOCOL**, **GOAL** and **BACKEND**: These sections specify the protocol name, goal of the analysis and the back-end used, respectively.

Several basic types are supported by HLPSL, the commonly used are [55]:

- *agent*: principal name. The intruder has always the special identifier i.
- *public_key*: represents agents' public keys.
- *symmetric_key*: represents a symmetric-key.
- *text*: represents nonces.

- *nat*: represents natural numbers used non-message contexts.
- *const*: represents constants.
- *hash_func*: represents a cryptographic collision-resistant one-way hash function.

6.1 Specifying our scheme in HLPSL

In the proposed protocol, there are two basic roles: MP MP and Wireless Sensor Networksserver CS. Both the roles have been specified in HLPSL. Apart from these basic roles, we have three other roles: the session, environment and goal.

```
role alice (MP,CS : agent,
            SKmpcs : symmetric key,
            %H is the one- way hash function
            %h is the perceptual Hashing function
            H : hash func,
            h : hash func,
            Snd, Rcv: channel(dy))
%Played by the initiator the medical professional MP
played_ by MP
def=
local State : nat,
            IDmp, PWmp, Bmp, T1, a, yamp: text
            Ramp, MID, Zmp, A : text
const alice_bob_t1, bob_alice_t3, alice_bob_r,
alice_bob_u, subs1, subs2, subs3 : protocol_id
init State := 0
transition
%medical professional registration phase

1. State = 0 /\ Rcv(start) =|>
  State':=1 /\ IDmp':= new()
            /\ PWmp':= new()
            /\ Bmp':= new()
            /\ BIOmp':=H(Bmp)
            /\ Snd({IDmp',PWmp',BIOmp'}_SKmpcs)
            /\ secret({IDmp',PWmp',BIOmp'},subsl,MP)
%Receive the registration acknowledgment message from CS

2.State = 1 /\ Rcv({Tmp',Rmp',Smp'})_SKmpcs)=|>
%Login phase
state':= 2
% Send the LOGIN REQUEST message to CS
  /\ a':= new()
  /\ T1':=new()
  /\ A'=exp(a',G)
  /\ yamp'=xor(xor(xor(PWmp',BIOmp'),IDmp'),Smp')
  /\ Ramp':=xor(H(xor(xor(IDmp',PWmp'),BIOmp')),H(ymp'))
  /\ X:=xor(Smp',H(IDmp'.PWmp'.BIOmp'))
  /\ MID':=H(xor(IDmp',yamp'),H(X))
  /\ Zmp':=H(IDmp'.H(X).yamp')
  /\ beta':=H(Zmp'.T1')
  /\ Snd({IDmp',MID',beta',T1'}_SKmpcs)
  /\ secret({IDmp',MID',beta',T1'},subs3,MP)
% MP has freshly generated the value a for CS
        /\ witness(MP,CS,alice_bob_mp,MP)
% MP has freshly generated the value T1 for CS
        /\ witness(MP,CS,alice_bob_t1,T1')
% Authentication phase

3. State = 5 /\ Rcv({Gacs',u',L',T2'}_SKmpcs)
end role
```

Figure 7. Role specification for the user MP

```
role alice (MP,CS : agent,
SKmpcs : symmetric_key,
%H is the one-way hash function
% h is the perceptual Hashing function
H : hash func,
h : hash func, Snd, Rcv: channel(dy))
% Played by the responder the cloud server CS
played_by CS
def=
local State : nat,
        IDmp, PWmp, Bmp, T1, a, yamp: text
      Ramp, MID, Zmp, A : text
      const alice_bob t1,bob_alice_t3,
        alice bob_cs, alice bob_mp, subsl, subs2, subs3 : protocol_id
init State := 0
transition
% User registration phase
% Receive the registration request message from Ui

1. State = 0 /\ Rcv({IDmp',PWmp',BIOmp'}_SKmpcs) =|>
            /\ ymp':=new()
            /\ Tmp':=xor(H(IDmp',PWmp',BIOmp'),H(X))
            /\ Rmp':=xor(H(IDmp', PWmp',BIOmp'),H(ymp'))
            /\ Smp':=xor(xor(xor(ymp',1Dmp'),PWmp'),BlOmp')
% Said the registration acknowledgment message to MP
            /\ Snd({Tmp',Rmp',Smp'}_SKmpcs)
            /\ secret({Tmp', Rmp',Smp'} ,subs2,{MP,CS})
            /\ Dmp':= H(xor(H(IDmp'.ymp'),x))
% Login phase
% Receive the REQUEST message

2. State= 2 /\ Rcv({IDmp',MID',beta',T1'}_SKmpcs)=|>
% Authentication phase
state' := 4 /\ Damp':=H(xor(MID',H(X)),X)
            /\ Zamp':=H(IDmp'.H(X).ymp')
            /\ betaa':=H(Zamp'.T1)
            /\ c':=exp(A,Xcs)
% CS has freshly generated the value T2 for MP
            /\ T2:=new()
            /\ L':=H(A.T2)
% CS has freshly generated the value u for MP
            /\ u':=new()
            /\ Gacs':=H(c.u.Zamp'.T2')
            /\ Snd({Gacs',u',L',T2'}_SKmpcs)
            /\ secret({Gacs',u',L',T2'},subs4,{MP,CS})
            /\ witness(CS, MP, bob_alice_T1,T1')
            /\ request(MP, CS, alice_bob_T1,T1')
end role
```

Figure 8. Role specification for the CS

Figure 7 specifies the role of the MP represented by MP. On receiving the start signal MP will change its state from 0 to 1, and send registration request message <IDmp,PWmp,Bmp> via secure channel to CS. To send the message to CS, it uses the Snd() operation. CS will then perform specified computations and through a secure channel sends the smart card issued for MP. During the login phase, MP will send the login message < IDmp,MID,beta,T1> to CS on an insecure public channel, and then waits for an authentication message <Gacs,u,L,t2> from CS using Rcv() operation. witness(MP, CS, alice_bob_t1, T1) declares that MP has freshly generated the timestamp T1 for CS. witness(MP, CS, alice_bob_a, a') declares that MP has freshly generated the nonce a for CS. request(CS, MP, bob_alice_t1, T1') indicates that MP's acceptance of the timestamp T1 generated by MP by CS in which MP authenticates CS. request(CS, MP, bob_alice_a, a') indicates that MP's acceptance of the nonce generated by MP for CS in which MP authenticates CS.

Figure 8 shows the implementation of the proposed protocol for the Wireless Sensor Networksserver CS. During the registration phase, after receiving the message <IDmp,PWmp,Bmp> on secure channel from MP, CS carries out required computations and then sends the smart card through secure channel to MP. CS will then receive the login request message <IDmp,MID,beta,T1 >. Subsequently, CS will send the authentication message <Gacs,u,L,T2> on an insecure public channel to MP as a reply to the received login message from MP.

Figure 9 and Figure 10 show the role specification for session, and for the goal and environment, respectively. In the session role, all basic roles including the roles for MP and CS are considered as the instances with concrete arguments. The environment role contains the global constants and a composition of one or more sessions. It is assumed that an intruder 'I' may also play some roles as the legitimate users. The intruder thus participates in the execution of a protocol as a concrete session. In our implementation, four secrecy goals and two authentications are verified, which are shown in Figure 10.

```
role session(MP, CS: agent,
      SKmpcs : sytnmetric key,
      H : hash fimc, h : hash func)
def=
local SI, SJ, RI, RJ: channel (dy)
composition
alice(MP, CS, SKmpcs, H, h, SI, RI)
/\bob (CS, MP, SKmpcs, H, h, SJ, RI)
end role
```

Figure 9. Role specification for the session

```
role environment()
def=
const MP,CS: agent,
SKmpcs : symmetric_key,
h: hash func,
H: hash_func,
alice_bob_T1,bob_alice_T2,alice_bob_a,
alice bob_u, subs1, subs2, subs3,subs4 : protocol_id
intruder_knowledge = {MP, CS, h, H}
composition
session(MP, CS, SKmpcs, H, h)
session(MP ,C,Ss ,SKmpcs,H,h)
end role
goal
secrecy_of subs1
secrecy_of subs2
secrecy_of subs3
secrecy_of subs4
authentication on alice_bob_ T1
authentication on bob_alice_T2
end goal
environment()
```

Figure 10. Role specification for the goal and environment

7 Conclusion

In this paper, we have proposed ECC based authentication protocol real time remote patient monitoring and tracking based on Wireless Sensor Networks-IOT environments. In the protocol, a MP can access in real time any remote patient's sensor data stored on a remote Wireless Sensor Networks server and based on the observed data he can take care of the registered patient. The proposed scheme satisfies all the desirable security requirements including mutual authentication, confidentiality, forward secrecy, scalability and integrity. We have simulated the scheme for formal security verification using the widely-accepted web based AVISPA tool and show that the proposed protocol is secure against passive and active attacks including the replay and man-in-the-middle attacks. In addition, the protocol maintains session key freshness at any time every time the Wireless Sensor Networks server is accessed by the MP. Also, the protocol sets up a symmetric secret session key between MP and Wireless Sensor Networks server for use in secure data access and communication. The performance analysis confirms that the proposed protocol is efficient as compared to other existing schemes in terms of computation costs, security requirements and resistance to several attacks.

References

[1] M. R. Abdmeziem and D. Tandjaoui, "An end-to-end secure key management protocol for e-health applications q," *Computers and Electrical Engineering*, vol. 44, pp. 184–197, 2015.

[2] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: securing sensor networks with public key technology," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, 2004, pp. 59–64.

[3] Z. Benenson, N. Gedicke, and O. Raivio, "Realizing robust user authentication in sensor networks," *Real-World Wireless Sensor Networks (REALWSN)*, vol. 14, p. 52, 2005.

[4] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)*, 2006, vol. 1, p. 8--pp.

[5] H.-R. Tseng, R.-H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference*, 2007, pp. 986–990.

[6] F. Hu, M. Jiang, M. Wagner, and D.-C. Dong, "Privacy-preserving telecardiology sensor networks: toward a low-cost portable wireless hardware/software codesign," *IEEE Transactions on Information Technology in Biomedicine*, vol. 11, no. 6, pp. 619–627, 2007.

[7] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[8] Y.-M. Huang, 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, 2009.

[9] K. Malasri and L. Wang, "Design and implementation of a securewireless mote-based medical sensor network," *Sensors*, vol. 9, no. 8, pp. 6273–6297, 2009.

[10] J. C. Sriram, M. Shin, T. Choudhury, and D. Kotz, "Activity-aware ECG-based patient authentication for remote health monitoring," in *Proceedings of the 2009 international conference on Multimodal interfaces*, 2009, pp. 297–304.

[11] N. D. Sarier, "Improving the accuracy and storage cost in biometric remote authentication schemes," *Journal of Network and Computer Applications*, vol. 33, no. 3, pp. 268–274, 2010.

[12] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 60–68, 2010.

[13] J. Yuan, C. Jiang, and Z. Jiang, "A biometric-based user authentication for wireless sensor networks," *Wuhan University Journal of Natural Sciences*, vol. 15, no. 3, pp. 272–276, 2010.

[14] T.-H. Chen, Y.-C. Chen, W.-K. Shih, and H.-W. Wei, "An efficient anonymous authentication protocol for mobile pay-TV," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1131–1137, 2011.

[15] X. H. Le, M. Khalid, R. Sankar, and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare," *Journal of Networks*, vol. 6, no. 3, pp. 355–364, 2011.

[16] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[17] H. Chen, L. Ge, and L. Xie, "A User Authentication Scheme Based on Elliptic Curves Cryptography for Wireless Ad Hoc Networks," *Sensors*, vol. 15, no. 7, pp. 17057–17075, 2015.

[18] E.-J. Yoon and K.-Y. Yoo, "A new biometric-based user authentication scheme without using password for wireless sensor networks," in *Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2011 20th IEEE International Workshops on*, 2011, pp. 279–284.

[19] W. Drira, E. Renault, and D. Zeghlache, "A hybrid authentication and key establishment scheme for wban," in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012, pp. 78–83.

[20] D. He, C. Chen, S. Chan, J. Bu, and A. V Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 4, pp. 623–632, 2012.

[21] P. Kumar, M. Ylianttila, A. Gurtov, S.-G. Lee, and H.-J. Lee, "An efficient and adaptive mutual authentication framework for heterogeneous wireless sensor network-based applications," *Sensors*, vol. 14, no. 2, pp. 2732–2755, 2014.

[22] Z. Zhang, H. Wang, A. V Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1070–1078, 2012.

[23] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, "An efficient biometric authentication protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[24] M. Barua, R. Lu, and X. Shen, "SPS: Secure personal health information sharing with patient-centric access control in Wireless Sensor Networkscomputing," in *2013 IEEE Global Communications Conference (GLOBECOM)*, 2013, pp. 647–652.

[25] K. Divi and H. Liu, "Modeling of WBAN and Wireless Sensor Networksintegration for secure and reliable healthcare," in *Proceedings of the 8th International Conference on Body Area Networks*, 2013, pp. 128–131.

[26] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Transactions on sensor Networks (TOSN)*, vol. 9, no. 2, p. 18, 2013.

[27] C. Lv, M. Ma, H. Li, J. Ma, and Y. Zhang, "An novel three-party authenticated key exchange protocol using one-time key," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 498–503, 2013.

[28] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: body area network authentication exploiting channel characteristics," *IEEE Journal on selected Areas in Communications*, vol. 31, no. 9, pp. 1803–1816, 2013.

[29] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 316–323, 2013.

[30] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[31] G. Almashaqbeh, T. Hayajneh, A. V Vasilakos, and B. J. Mohd, "QoS-aware health monitoring system using cloud-based WBANs," *Journal of medical systems*, vol. 38, no. 10, pp. 1–20, 2014.

[32] N. D. Han, L. Han, D. M. Tuan, H. P. In, and M. Jo, "A scheme for data confidentiality in cloud-assisted wireless body area networks," *Information sciences*, vol. 284, pp. 157–166, 2014.

[33] D. Mishra, J. Srinivas, and S. Mukhopadhyay, "A secure and efficient chaotic map-based authenticated key agreement scheme for telecare medicine information systems," *Journal of medical systems*, vol. 38, no. 10, pp. 1–10, 2014.

[34] Z. Tan, "A user anonymity preserving three-factor authentication scheme for telecare medicine information systems," *Journal of medical systems*, vol. 38, no. 3, pp. 1–9, 2014.

[35] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem, "A platform for secure monitoring and sharing of generic health data in the Cloud," *Future Generation Computer Systems*, vol. 35, pp. 102–113, 2014.

[36] J. Xu, W.-T. Zhu, and D.-G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[37] Z. Zhao, "An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem," *Journal of medical systems*, vol. 38, no. 2, pp. 1–7, 2014.

[38] S. Ullah, M. Imran, and M. Alnuem, "A hybrid and secure priority-guaranteed MAC protocol for wireless body area network," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[39] H. Yang, H. Kim, and K. Mtonga, "An efficient privacy-preserving authentication scheme with adaptive key evolution in remote health monitoring system," *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1059–1069, 2015.

[40] S. K. Shankar, A. S. Tomar, and G. K. Tak, "Secure Medical Data Transmission by Using ECC with Mutual Authentication in WSNs," *Procedia Computer Science*, vol. 70, pp. 455–461, 2015.

[41] Z. Quan, T. Chunming, Z. Xianghan, and R. Chunming, "A secure user authentication protocol for sensor network in data capturing," *Journal of Wireless Sensor NetworksComputing*, vol. 4, no. 1, pp. 1–12, 2015.

[42] Y. Lu, L. Li, H. Peng, and Y. Yang, "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem," *Journal of Medical Systems*, vol. 39, no. 3, pp. 1–8, 2015.

[43] H. Arshad and M. Nikooghadam, "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems," *Journal of medical systems*, vol. 38, no. 12, pp. 1–12, 2014.

[44] M. S. Hossain and G. Muhammad, "Cloud-assisted speech and face recognition framework for health monitoring," *Mobile Networks and Applications*, vol. 20, no. 3, pp. 391–399, 2015.

[45] R. Amin and G. P. Biswas, "A secure three-factor user authentication and key agreement protocol for tmis with user anonymity," *Journal of medical systems*, vol. 39, no. 8, pp. 1–19, 2015.

[46] X. Xu, P. Zhu, Q. Wen, Z. Jin, H. Zhang, and L. He, "A secure and efficient authentication and key agreement scheme based on ecc for telecare medicine information systems," *Journal of medical systems*, vol. 38, no. 1, pp. 1–7, 2014.

[47] C. Liu and Y. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," vol. 0, pp. 1–12, 2016.

[48] S. R. Moosavi *et al.*, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Generation Computer Systems*, vol. 64, pp. 108–124, 2016.

[49] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, and J. Shen, "A lightweight and anonymous RFID tag authentication protocol with Wireless Sensor Networksassistance for e-healthcare applications," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–12, 2017.

[50] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," *Journal of Information Security and Applications*, 2017.

[51] C.-T. Li, T.-Y. Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, "An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT-Based Medical Care System," *Sensors*, vol. 17, no. 7, p. 1482, 2017.

[52] P. K. Dhillon and S. Kalra, "Secure multi-factor remote user authentication scheme for Internet of Things environments," *International Journal of Communication Systems*, 2017.

[53] G. Góodor, P. Szendi, and S. Imre, "Elliptic curve cryptography based authentication protocol for small computational capacity RFID systems," in *Proceedings of the 6th ACM Workshop on QoS and Security for Wireless and Mobile Networks*, 2010, pp. 98–105.

[54] X. Niu and Y. Jiao, "An overview of perceptual hashing," *Acta Electronica Sinica*, vol. 36, no. 7, pp. 1405–1411, 2008.

[55] A. Armando, D. Basin, J. Cuellar, M. Rusinowitch, and L. Viganò, "AVISPA: Automated Validation of Internet Security Protocols and Applications," *ERCIM News*, vol. 64, 2006.