International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

A NOVEL SECURE WIRELESS HEALTHCARE APPLICATIONS FOR MEDICAL COMMUNITY

Mohammed Alshehri [a*]

[a] *College of Computer and Information Sciences, Majmaah University, Majmaah-11952, SAUDI ARABIA*

ARTICLEINFO

Article history:
Received 07 January 2019
Received in revised form 05 March 2019
Accepted 08 March 2019
Available online
08 March 2019

Keywords:
Community Cloud for Healthcare (CCH); Community Cloud of Certifying Authority (CCCA); Wireless Medical Sensor Networks (WMSN); Scyther tool; BAN logic.

ABSTRACT

The exponential advancements in the realm of wearable biosensor and wireless communication technologies has paved the way to a new technology called Wireless Medical Sensor Networks (WMSNs) which is revolutionizing mobile healthcare. This work is motivated from ABI research report that all the healthcare infrastructures are prone to attacks which includes Cloud, IOT Wearable Devices, Mobile Network Operator (MNO) and Secure Element (SE) of the patient. There are many challenges in implementation including adversaries exploiting vulnerabilities in Information and Communication Technologies (ICT) thereby compromising patient's vital information. This article proposes a Secure and Anonymous Health (SAH) Monitoring System using Wireless Medical Sensor Networks (WMSN). SAH overcomes all the flaws in the existing literature by adopting Community Cloud for Healthcare (CCH) and Community Cloud of Certifying Authority (CCCA). SAH framework ensures all the security properties and withstands all the known attacks. SAH protocol is verified with scyther tool and BAN logic so we claim that SAH framework ensures all the security properties such as confidentiality, integrity, non-repudiation, and authentication are ensured and withstands all the known attacks which includes multi-protocol attacks.

1. INTRODUCTION

The exponential advancements in the realm of wearable biosensor and wireless communication technologies has paved the way to a new technology called Wireless Medical Sensor Networks (WMSNs) which is revolutionizing mobile healthcare. Using WMSN patients 'health-related parameters can be monitored remotely in the real time and transferred to hospital thereby increasing the efficiency of health services. Adopting Mobile cloud computing (MCC) in the healthcare will enhance the services. But there are many challenges in implementation of these services which includes adversaries exploiting vulnerabilities in Information and Communication Technologies (ICT) thereby compromising patient's vital information. So to overcome these challenges we propose a Secure and Anonymous Health (SAH) Monitoring System using Wireless Medical Sensor Networks (WMSN). SAH overcomes all the flaws in the existing literature by adopting Community Cloud for Healthcare (CCH) and Community Cloud of Certifying Authority (CCCA). SAH framework ensures all the security properties and withstands all the known attacks. This article is organized in sections, section 2 is about Methods in the SAH system, section 3 provides results using scythe tool and BAN logic, section 4 provides discussion. We have observed very few publications/works in the literature of mobile health-care over Wireless Medical Sensor Networks (WMSN) proposing secure framework in mobile healthcare systems, but there are many publications/works in the literature such as which only focuses on authentication only but never ensures security framework. This paper ensures security in the realm of mobile healthcare so we consider only (Ruhul Amina & Hafizul Islam, 2018; Khan & Kumari, 2014) as related work for our proposed framework.

Following are the limitations in the proposed model:

a) Proposed scheme does not ensure Non-repudiation property.
b) There is no clarity how data is secured in the cloud
c) There is no clarity how privacy is ensured in the scheme
d) There is no clarity how HIPAA standard is implemented
e) Prone to multi-protocol attacks
f) Formal verification is not done

Following are the limitations in the security model proposed:

a) Proposed scheme doesn't ensure Non-repudiation property
b) There is no clarity how data is secured in the cloud
c) There is no clarity how privacy is ensured in the scheme
d) There is no clarity how HIPAA standard is implemented
e) Prone to multi-protocol attacks

The paper have the following objectives:

a) We have proposed a secure and anonymous health monitoring system architecture used for WMSN as shown in the figure 1 ensuring end to end security and consumes fewer resources.
b) We have proposed protocols for personalizing the sensor node, health monitoring mobile application (in UICC) and healthcare application in the Community Cloud for Healthcare (CCH), which ensures all the security properties including patient anonymity for Doctors.
c) We have used Scyther tool in order verify our proposed protocol and found to be safe and is free from any type of attacks (which include active and passive attacks).
d) Our proposed protocol overcomes all the known attacks in addition to Multi-Protocol attacks as our proposed protocol is successfully verified using BAN logic and Scyther (Kumar et al, 2013).

2. METHODS

2.1 Stakeholders in the SAH System

Following are the stakeholders

a) **IOT Wearable Device (WD):** This device contains a Secure Element (SE) and a healthcare application in the SE, which is personalized by the Patient (P).

b) **UICC (UC):** UICC is the secure element in the mobile phone of patient.

c) **Mobile Network Operator (MNO):** This entity provides network connectivity OTA (Over The Air).

d) **Doctor: D is** assumed with mobile phone having a Secure Element (SE) in our proposed system.

e) **Patient: P is** assumed with mobile phone having a Secure Element (SE) in our proposed system.

f) **Community Cloud for Healthcare (CCH):** CCH is a Community Cloud of all the hospitals in the country under the supervision of Regulatory Authority such as CHA (Central Healthcare Authority). CCH allocates one HSM (Hardware Security Module) for each hospital in order to keep their data. Following are the components of CCH (Li et al, 2015).

2.2 Authentication Manager (AM)

This entity authenticates all the stakeholders I the ecosystem by their credentials issued by CA/TSM.

a. **Communication Manager (CM):** CM ensures end to end reliable communication security using SSL/TLS.
b. **Time Stamping Authority (TSA):** TSA performs Time stamping and nonce services in CCA.
c. **Personalization Manager (PM)**: PM personalizes mobile healthcare applications of patients and doctors. PM manages the credentials of all the stakeholders including public keys and symmetric keys.
d. **Auditor:** Auditor acts as an adjudicator, it keeps a copy of the evidence. Auditor presents these evidences in the court.
e. **Community Cloud of Certifying Authority (CCCA):** CCCA is the community cloud of the CA (Certifying Authority), it supports both Wireless PKI and PKI. CCCA has the Registration Authority (RA), Time Stamping Authority and Directory. CCCA supports OCSP service and generates and manages Certificates (Wu et al, 2015).

3. RESULTS AND DISCUSSION

3.1 Registration Phase

a) Step 1: Hospital (H) is the Registration Authority (RA) and verifies the credentials. Credentials include Secure Elements and National Identities. After successful verification it recommends CA to issue Anonymous certificates for patients and doctors. Patients and doctors generate their credentials using the

*Corresponding author (Mohammed Alshehri). Tel: +966-16404-6767. E-mail: ma.alshehri@mu.edu.sa

procedure given in (Shaik Shakeel Ahamad et al, 2014). These certificates are mapped with the Secure Element certificate and National Identity.

b) **Step 2:** Traceable Anonymous Certificate (TAC's) are issued to Patient (P) as per the RFC 5636 (Cremers, 2006: Xu & Wu, 2015).

c) **Step 3:** Mobile Healthcare Application is downloaded and installed on the SE by both Doctor (D) and Patient (P).

3.2 Personalization Phase

IoT wearable device has a Secure Element (SE) and a healthcare application. IoT wearable device is issued by the hospital with unique identity of the device. CA issues a certificate for both Secure Element (SE) and healthcare application in IoT wearable device. IoT wearable device will only communicate with the healthcare application in the UICC of patient's mobile phone using Bluetooth low energy. Healthcare application in the UICC and Healthcare application in IoT wearable device share the same secret Key where W= IoT wearable device and P= Patient. Healthcare application in IoT wearable device is personalized by the Healthcare application in the UICC. Healthcare application in IoT wearable device will only communicate with the Healthcare application in the UICC. Body Sensor Networks (BSN) collects patient's data and sends to the UICC of the patient in an encrypted form with an interval of 5 to 10 min using Bluetooth low energy. Symmetric key shared between Healthcare application in the UICC and IoT wearable device is used to encrypt messages. The patient's data is sent by the BSN in encrypted form by encrypting the data with the shared symmetric between IoT wearable sensor and the healthcare application in the UICC. Following are the steps involved in the Personalization of Mobile healthcare application by CCH. Figure 2 depicts these steps

Step 1: Patient downloads healthcare application from CCH

Step 2: CCH personalizes patient's healthcare application installed in the UICC

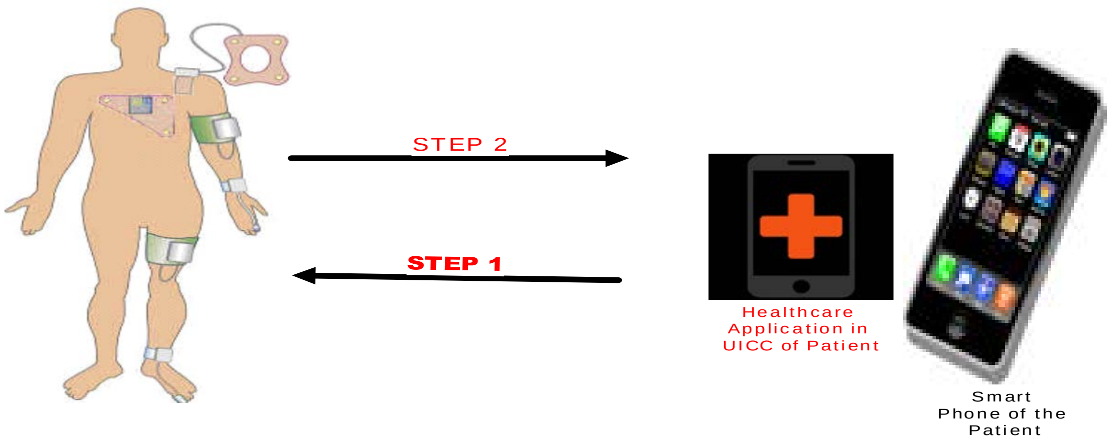

Figure 1: Personalization of Healthcare Application in IOT Wearable Device by the Patient.

3.3 PERSONALIZATION PHASE

IoT wearable device has a Secure Element (SE) and a healthcare application. IoT wearable device is issued by the hospital with unique identity of the device. CA issues a certificate for both Secure Element (SE) and healthcare application in IoT wearable device. IoT wearable device will only communicate with the healthcare application in the UICC of patient's mobile phone using Bluetooth low energy. Healthcare application in the UICC and Healthcare application in IoT wearable device share the same secret Key $\mathbf{SYYKEY_{WP}}$ where W= IoT wearable device and P= Patient. Healthcare application in IoT wearable device is personalized by the Healthcare application in the UICC. Healthcare application in IoT wearable device will only communicate with the Healthcare application in the UICC. Body Sensor Networks (BSN) collects patient's data and sends to the UICC of the patient in an encrypted form with an interval of 5 to 10 min using Bluetooth low energy. Symmetric key shared between Healthcare application in the UICC and IoT wearable device is used to encrypt messages. The patient's data is sent by the BSN in encrypted form by encrypting the data with the shared symmetric between IoT wearable sensor and the healthcare application in the UICC. Following are the steps involved in the Personalization of Mobile healthcare application by CCH. Figure 2 depicts these steps.

Step 1: Patient downloads healthcare application from CCH

Step 2: CCH personalizes patient's healthcare application installed in the UICC

Step 2a.

$\boldsymbol{Step\ 1: UC \rightarrow CCH: \{MS1, SIG\{MS1\}_{PrKEY_{UC}}\},\ Cert_{uc}}$

$\boldsymbol{MS1: \{PID, Phno, NRP, T_{uc}, N_{uc}\}}$

/* In order to personalize mobile healthcare application in UICC mutual authentication between UICC and CCH should be ensured.*/

Step 2b.

$$Step2: \mathrm{MCS} \rightarrow P: \{MS2, SIG_P^{MCS}(MS2)\}_{k_p}, cert_{MCS}$$

$$MS2 = \{\mathrm{PID}, phno, K_{mp}, N_{mcs}, T_{mcs}, N_p\}$$

$\boldsymbol{Step\ 2: CCH \rightarrow UC: \{MS2, SIG\{MS2\}_{PrKEY_{cch}}\}}$

$\boldsymbol{MS2: \{PID, Phno, SYYKEY_{uccch}, T_{uc}, N_{uc}, T_{cch}, N_{cch}\}}$

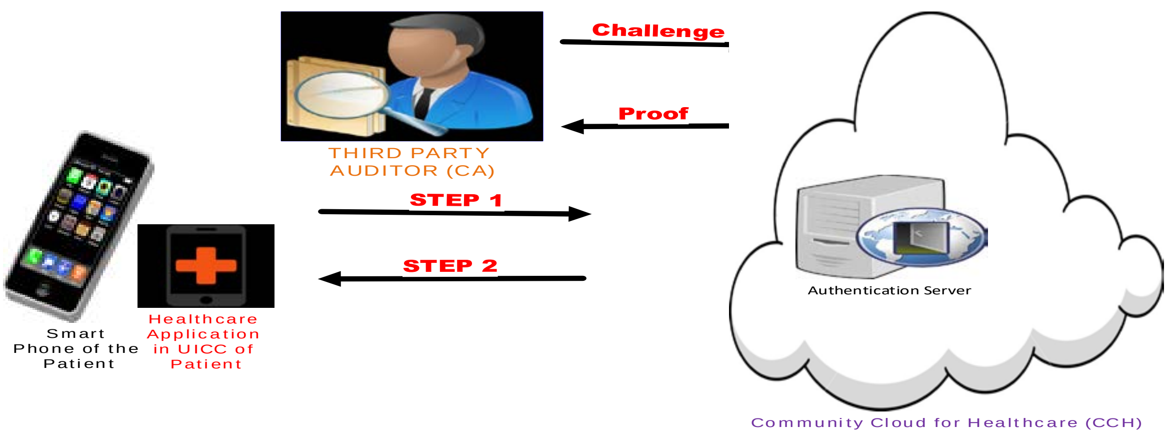

Figure 2: Personalization of Healthcare Application in the UICC by CCH

Following is the proposed Secure and Anonymous Healthcare (SAH) Protocol. Figure 3 depicts these steps

$$\boldsymbol{Step\ 1}: \boldsymbol{WD} \rightarrow \boldsymbol{UC}: \{\boldsymbol{MS1}\}$$

$$\boldsymbol{MS1}: \{\boldsymbol{PLoc}, \boldsymbol{sensorreading}.\boldsymbol{T_{wd}}, \boldsymbol{N_{wd}}\}$$

$$\boldsymbol{Step\ 2}: \boldsymbol{UC} \rightarrow \boldsymbol{WD}: \{\boldsymbol{MS2}\}$$

$$\boldsymbol{MS2}: \{\boldsymbol{Ack}.\boldsymbol{PLoc}, \boldsymbol{sensorreading}.\boldsymbol{T_{uc}}, \boldsymbol{N_{uc}}, \boldsymbol{T_{wd}}, \boldsymbol{N_{wd}}\}$$

$$\boldsymbol{Step\ 3}: \boldsymbol{UC} \rightarrow \boldsymbol{CCH}: \{\boldsymbol{MS3}\}_{\boldsymbol{SYYKEY_{HP}}}$$

$$\boldsymbol{MS2}: \{\boldsymbol{PLoc}, \boldsymbol{PID}, \boldsymbol{sensorreading}, \boldsymbol{T_{uc}}, \boldsymbol{N_{uc}}, \boldsymbol{T_{wd}}, \boldsymbol{N_{wd}}\}$$

$$\boldsymbol{Step\ 4}: \boldsymbol{CCH} \rightarrow \boldsymbol{D}: \{\boldsymbol{MS4}\}_{\boldsymbol{SYYKEY_{HD}}}$$

$$\boldsymbol{MS3}: \{\boldsymbol{PLoc}, \boldsymbol{PID}, \boldsymbol{sensorreading}, \boldsymbol{T_{cch}}, \boldsymbol{N_{cch}}, \boldsymbol{T_{uc}}, \boldsymbol{N_{uc}}, \boldsymbol{T_{wd}}, \boldsymbol{N_{wd}}\}$$

$$\boldsymbol{Step\ 5}: \boldsymbol{CCH} \rightarrow \boldsymbol{CHA}: \{\boldsymbol{MS5}\}_{\boldsymbol{SYYKEY_{HCHA}}}$$

$$\boldsymbol{MS4}: \{\boldsymbol{PID}, \boldsymbol{PLoc}, \boldsymbol{sensorreading}, \boldsymbol{T_{cch}}, \boldsymbol{N_{cch}}, \boldsymbol{T_{uc}}, \boldsymbol{N_{uc}}, \boldsymbol{T_{wd}}, \boldsymbol{N_{wd}}\}$$

$$\boldsymbol{Step\ 1}: \boldsymbol{WD} \rightarrow \boldsymbol{UICC}: \{\boldsymbol{MS1}\}$$

$$\boldsymbol{MS1}: \{\boldsymbol{PLoc}, \boldsymbol{sensorreading}.\boldsymbol{T_S}, \boldsymbol{N_S}\}$$

Step 1: IOT Wearable Device (WD) sends the sensor readings of patient to UICC along with the location of patient.

$$\boldsymbol{Step\ 2}: \boldsymbol{UICC} \rightarrow \boldsymbol{CCH}: \{\boldsymbol{MS2}\}_{\boldsymbol{SYYKEY_{HP}}}$$

$$\boldsymbol{MS2}: \{\boldsymbol{PLoc}, \boldsymbol{PID}, \boldsymbol{sensorreading}, \boldsymbol{T_P}, \boldsymbol{N_P}\}$$

Step 2: UICC sends MS2 to CCH by encrypting with the symmetric shared between UICC and CCH.

$$\boldsymbol{Step\ 3}: \boldsymbol{CCH} \rightarrow \boldsymbol{D}: \{\boldsymbol{MS3}\}_{\boldsymbol{SYYKEY_{HD}}}$$

$$\boldsymbol{MS3}: \{\boldsymbol{PLoc}, \boldsymbol{PID}, \boldsymbol{sensorreading}, \boldsymbol{T_P}, \boldsymbol{N_P}, \boldsymbol{T_H}, \boldsymbol{N_H}\}$$

Step 3: CCH sends MS3 to D by encrypting with the symmetric shared between Doctor and CCH. CCH sends the shared key to the Doctor allocated in case of an emergency. Message also contains Timestamp, Nonce and PID (Patient Identity).

$$\boldsymbol{Step\ 4}: \boldsymbol{CCH} \rightarrow \boldsymbol{CHA}: \{\boldsymbol{MS4}\}_{\boldsymbol{SYYKEY_{HCHA}}}$$

$$\boldsymbol{MS4}: \{\boldsymbol{PID}, \boldsymbol{PLoc}, \boldsymbol{sensorreading}, \boldsymbol{T_P}, \boldsymbol{N_P}, \boldsymbol{T_H}, \boldsymbol{N_H}\}\}$$

Step 4: CCH sends MS4 to CHA by encrypting with the symmetric shared between CCH and CHA.

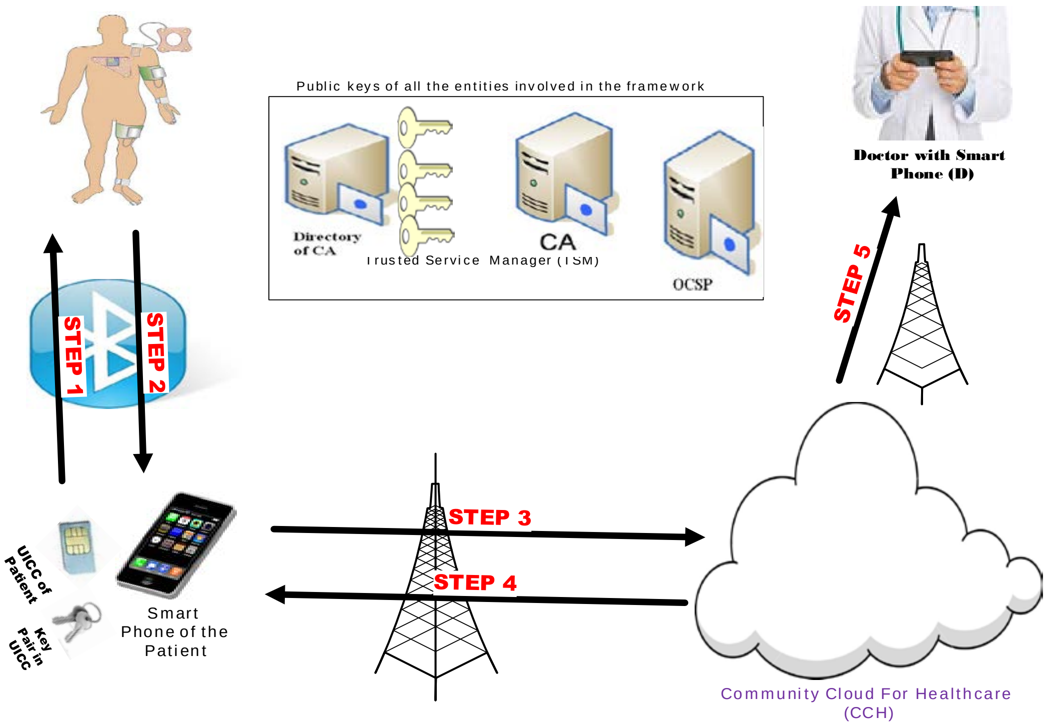

Figure 3: Steps involved in SAH Protocol.

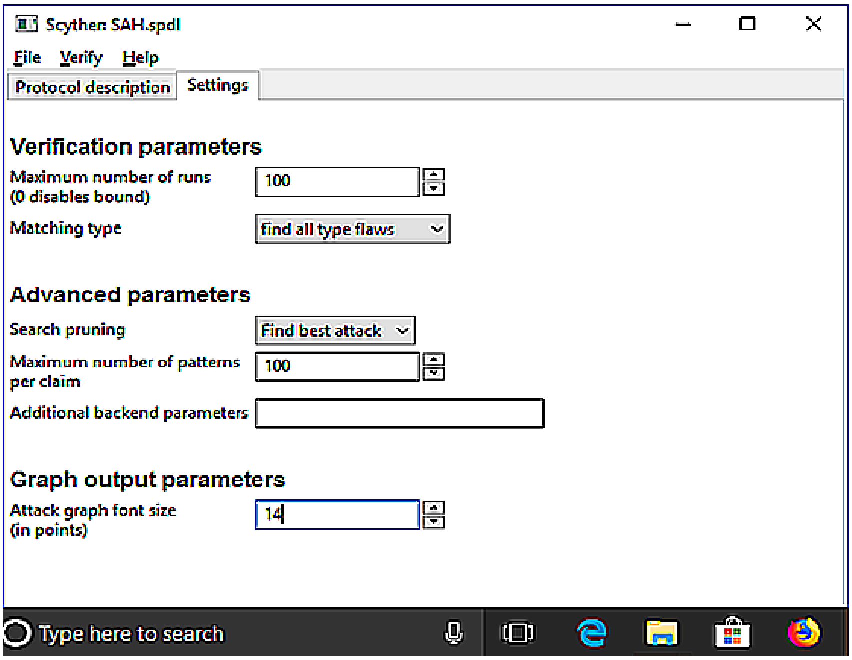

Figure 4: Parameters of SAH Protocol using Scyther Tool

SAH uses Scyther tool for verifying the proposed protocol. Scyther provides reliable simulation environment. SPDL (Security Protocol Description Language) is used to write code in Scyther tool. Following are the motivations in selecting Scyther tool compared to AVISPA tool (Armando, et al, 2005: Muhammad et al, 2006).

a) This tool assumes that each and every protocol runs with other protocols in the same network.

b) It uses SPDL language

c) Good in verifying Multi-Protocol attacks

d) When attacks are found in the protocol attack graphs are generated

e) Verification of protocols in scyther tool is done by bounded/unbounded number of sessions.

f) Unbounded or bounded number of sessions are supported in scyther tool

Table 1: Differences between AVISPA and Scyther tool

AVISPA Tool	Scyther Tool
Assumes that every protocol runs in isolation.	Assumes all the protocols runs with other protocols in the same network.
HLPSL language is used	SPDL language is used
Multi-Protocol attacks are not verified	Multi-Protocol attacks are verified
Attack graphs are not generated	When attacks are found attack graphs are created by scyther tool
Verification of protocols are done using only bounded number of sessions.	Verification of protocols are done by bounded/unbounded number of sessions.

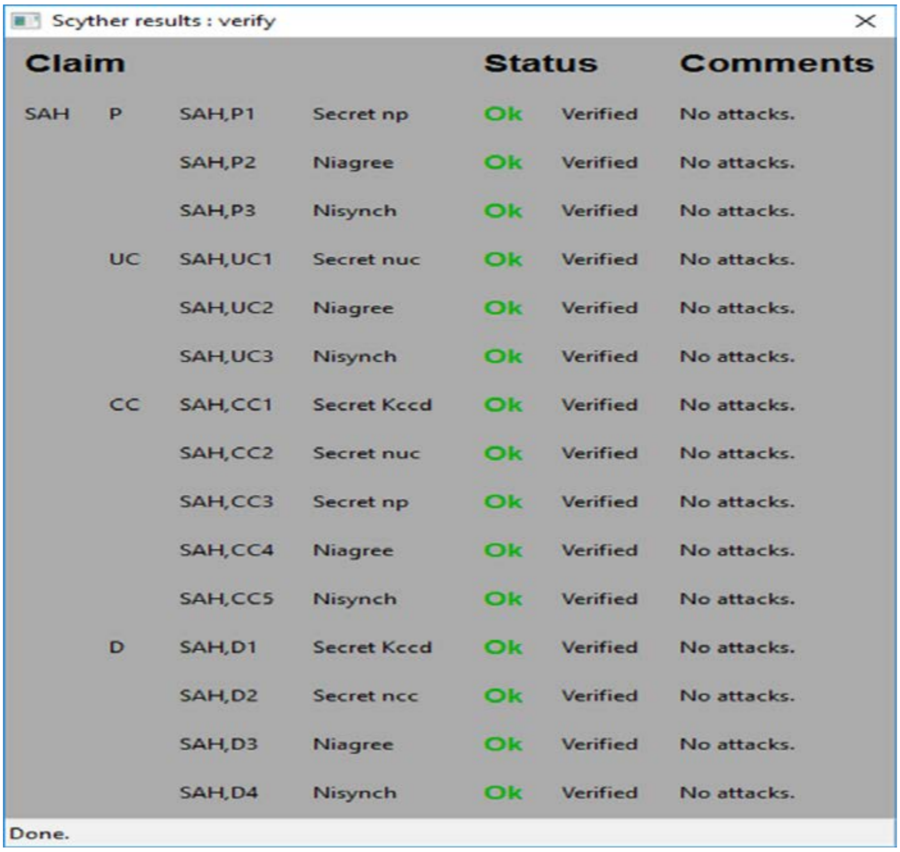

Figure 5: Result of SAH Protocol using “Verification Claim” Procedure of Scyther Tool.

3.4 BAN Logic Proof and Security Analysis

Protocols designed perfectly in the past were found to be error prone (Abadi et al, 1993). Authentication and correctness of the SAH protocol is verified using BAN logic (Burrows et al, 1990).

$$\boldsymbol{Step\ 1: WD \rightarrow UC: \{MS1\}}$$
$$\boldsymbol{MS1: \{PLoc, sensorreading. T_{wd}, N_{wd}\}}$$

$$\boldsymbol{Step\ 2: UC \rightarrow WD: \{MS2\}}$$
$$\boldsymbol{MS2: \{Ack. PLoc, sensorreading. T_{uc}, N_{uc}, T_{wd}, N_{wd}\}}$$

$$\boldsymbol{Step\ 3: UC \rightarrow CCH: \{MS3\}_{SYYKEY_{HP}}}$$
$$\boldsymbol{MS2: \{PLoc, PID, sensorreading, T_{uc}, N_{uc}, T_{wd}, N_{wd}\}}$$

SAH	P	SAH,P4	Secret Kucp	Ok	Verified	No attacks.
		SAH,P5	Secret np	Ok	Verified	No attacks.
		SAH,P6	Alive	Ok	Verified	No attacks.
		SAH,P7	Weakagree	Ok	Verified	No attacks.
		SAH,P8	Niagree	Ok	Verified	No attacks.
		SAH,P9	Nisynch	Ok	Verified	No attacks.
	UC	SAH,UC4	Secret Kuccc	Ok	Verified	No attacks.
		SAH,UC5	Secret Kucp	Ok	Verified	No attacks.
		SAH,UC6	Secret nuc	Ok	Verified	No attacks.
		SAH,UC7	Secret np	Ok	Verified	No attacks.
		SAH,UC8	Alive	Ok	Verified	No attacks.
		SAH,UC9	Weakagree	Ok	Verified	No attacks.
		SAH,UC10	Niagree	Ok	Verified	No attacks.
		SAH,UC11	Nisynch	Ok	Verified	No attacks.
	CC	SAH,CC6	Secret Kccd	Ok	Verified	No attacks.
		SAH,CC7	Secret Kuccc	Ok	Verified	No attacks.
		SAH,CC8	Secret ncc	Ok	Verified	No attacks.
		SAH,CC9	Secret nuc	Ok	Verified	No attacks.

Done.

Figure 6: Result of SAH Protocol using "Automatic Claim" Procedure of Scyther Tool

$$\boldsymbol{Step\ 4}: \boldsymbol{CCH} \rightarrow \boldsymbol{D}: \{\boldsymbol{MS4}\}_{\boldsymbol{SYYKEY_{HD}}}$$

$$\boldsymbol{MS3} : \{\boldsymbol{PLoc}, \boldsymbol{PID}, \boldsymbol{sensorreading}, \boldsymbol{T_{cch}}, \boldsymbol{N_{cch}}, \boldsymbol{T_{uc}}, \boldsymbol{N_{uc}}, \boldsymbol{T_{wd}}, \boldsymbol{N_{wd}}\}$$

$$\boldsymbol{Step\ 5}: \boldsymbol{CCH} \rightarrow \boldsymbol{CHA}: \{\boldsymbol{MS5}\}_{\boldsymbol{SYYKEY_{HCHA}}}$$

$$\boldsymbol{MS4} : \{\boldsymbol{PID}, \boldsymbol{PLoc}, \boldsymbol{sensorreading}, \boldsymbol{T_{cch}}, \boldsymbol{N_{cch}}, \boldsymbol{T_{uc}}, \boldsymbol{N_{uc}}, \boldsymbol{T_{wd}}, \boldsymbol{N_{wd}}\}$$

3.5 ASSUMPTIONS

3.5.1 SECRETS AND KEYS

CA contains all the certificates (valid) of all the participants **(AS1, AS2)**.

AS1. All the participants knows their own certificates

AS2. $S \in \{WD, \mathrm{UC, CCH, D\ and\ CA}\}$ S **believes** $\overset{K_{ca}}{\mapsto} CA)$. CA's certificate is with all the participants.

3.5.2 FRESHNESS

AS3 signifies freshness and AS4 signifies validity period of X.509 certificates

AS3. WD believes freshness$(\boldsymbol{N_{wd}})$ **, CCH believes freshness** $(\boldsymbol{N_{cch}})$**, UC believes freshness** $(\boldsymbol{N_{uc}})$**.**

AS4. TS_x& TS_y signifies time stamps

*Corresponding author (Mohammed Alshehri). Tel: +966-16404-6767. E-mail: ma.alshehri@mu.edu.sa

3.5.3 TRUST

AS5. CA is trusted by all the participants.

AS6. IoT Sensor transmits encrypted data and is trusted by CA.

AS7. Certification Authority (CA) believes that W/UICC relays Patient's beliefs.

3.5.4 VERIFICATION OF SAH

$\boldsymbol{Step\ 1: WD \rightarrow UC: \{MS1\}}$

$\boldsymbol{MS1: \{PLoc, sensorreading. T_{wd}, N_{wd}\}}$

UC decrypts the received $\{\boldsymbol{MS1}\}_{\boldsymbol{SYYKEY_{PUC}}}$

UC believes $\{\boldsymbol{MS1}\}_{\boldsymbol{SYYKEY_{PUC}}}$ statement (1)

UC checks P's certificate (**AS7**)

After successful verification

UC **believes fresh** N_p from **AS4** statement (2)

UC **believes P said** $\{\boldsymbol{MS1}\}_{\boldsymbol{SYYKEY_{PUC}}}$ statement (3)

UC **believes fresh** T_P from **AS3** statement (4)

UC believes $\{\boldsymbol{MS1}\}_{\boldsymbol{SYYKEY_{PUC}}}$

$\boldsymbol{Step\ 2: UC \rightarrow WD: \{MS2\}}$

$\boldsymbol{MS2: \{Ack. PLoc, sensorreading. T_{uc}, N_{uc}, T_{wd}, N_{wd}\}}$

UC receives the MS1 message from WD and sends MS2 message with an acknowledgement to WD. statement (5)

$\boldsymbol{Step\ 3: UC \rightarrow CCH: \{MS3\}_{SYYKEY_{UCCCH}}}$

$\boldsymbol{MS2: \{PLoc, PID, sensorreading, T_{uc}, N_{uc}, T_{wd}, N_{wd}\}}$

UC sends MS3 message encrypted with the symmetric key shared between UC and CCH. statement (6)

$\boldsymbol{Step\ 4: CCH \rightarrow D: \{MS4\}_{SYYKEY_{HD}}}$

$\boldsymbol{MS3: \{PLoc, PID, sensorreading, T_{cch}, N_{cch}, T_{uc}, N_{uc}, T_{wd}, N_{wd}\}}$

CCH decrypts the received message MS3

CCH **believes** $\{\boldsymbol{MS3}\}_{\boldsymbol{SYYKEY_{UCCCH}}}$ statement (7)

CCH checks UC's certificate (**AS7**)

After successful verification

CCH **believes UC said** $\{\boldsymbol{MS3}\}_{\boldsymbol{SYYKEY_{UCCCH}}}$ statement (8)

CCH believes **fresh** $\boldsymbol{T_{uc}, N_{uc}}$ from **AS4 & AS3** statement (9)

CCH believes $\{\boldsymbol{MS3}\}_{\boldsymbol{SYYKEY_{UCCCH}}}$

Doctor (D) verifies the received message as follows

D decrypts the received message MS4 from CCH

D **believes** $\{MS4\}_{SYYKEY_{HD}}$ statement (10)

D checks D's certificate (**AS7**)

D trusts $MS4$

$Step\ 5: CCH \rightarrow CHA: \{MS5\}_{SYYKEY_{HCHA}}$

$MS5 : \{PID, PLoc, sensorreading, T_{cch}, N_{cch}, T_{uc}, N_{uc}, T_{wd}, N_{wd}\}$

CHA decrypts the received message MS5 from CCH

CHA **believes** $\{MS5\}_{SYYKEY_{HCHA}}$

CHA checks CCH's certificate (**AS7**)

CHA believes $\{MS5\}_{SYYKEY_{HCHA}}$

3.6 ASSUMPTIONS

Following are the assumptions

Assumption 1: In our proposed system IOT Wearable Device (WD) is issued by the manufacturer to the Hospital. Hospital gets certificate from CA for the Secure Element (SE) embedded in the WD. Before issuing WD to the patient hospital maps WD's certificate with the certificate of the patient.

Assumption 2: In our proposed SAH system all the participants trust CA. TAC ensures anonymity for the Patient.

Assumption 3: TAC ensures anonymity for the Patient.

Assumption 4: Patient generates his own credentials in the secure area of secure element. ECDSA algorithm is used to digitally sign the messages

Assumption 5: Patient's and doctor's Application is personalized by the Community Cloud for Healthcare (CCH).

3.7 PROOFS OF SAH

Proposition 1: *Healthcare Application (HA) in UICC is personalized by the CCH*

Proof: Procedure is used by CCH Server to personalize Healthcare Application in the UICC

Proposition 2: *Messages exchanged among the participants during the transmission cannot be intercepted by the intruder*

Proof: In SAH system messages are exchanged in encrypted form and digitally signed using ECDSA algorithm.

Proposition 3: *Anonymity of the patient is ensured;*

Proof: CA issues TAC which ensures anonymity of the patient

Proposition 4*: Patient consumes fewer resources in SAH*

Proof: Patient uses digital signature based on ECDSA and the communication cost of the patient is very less.

Proposition 5: *SAH system ensures communication security*

Proof: SSL/TLS protocol is used in order to ensure communication security

Proposition 6: *SAH system generates Qualified Electronic Signatures*

Proof: CCH also uses TPM (Trusted Platform Module) which is considered as SSCD and UICC is also SSCD.So SAH generates Qualified Electronic Signatures.

Proposition 7: *SAH system withstands all the known attacks*

Proof: SAH protocol has been successfully verified using Scyther tool so SAH overcomes all the known attacks.

4. SUMMARY

The exponential advancements in the realm of wearable biosensor and wireless communication technologies has paved the way to a new technology called Wireless Medical Sensor Networks (WMSNs) which is revolutionizing mobile healthcare. This work is motivated from ABI research report that all the healthcare infrastructures are prone to attacks which includes Cloud, IOT Wearable Devices, Mobile Network Operator (MNO) and Secure Element (SE) of the patient. There are many challenges in implementation including adversaries exploiting vulnerabilities in Information and Communication Technologies (ICT) thereby compromising patient's vital information. This article proposes a Secure and Anonymous Health (SAH) Monitoring System using Wireless Medical Sensor Networks (WMSN). SAH overcomes all the flaws in the existing literature by adopting Community Cloud for Healthcare (CCH) and Community Cloud of Certifying Authority (CCCA). SAH protocol is verified with scythe tool and BAN logic. SAH framework ensures all the security properties and withstands all the known attacks.

Comparative analysis of SAH with related works is given in Table 2.

Table 2: Comparative Analysis of SAH with the Literature

Functionality/Features \ Protocols	Khan, and Kumari (2014)	Amin et al. (2018)	SAH (Our Proposed)
Personalization of IOT Wearable Device by the Patient	No	No	Yes
Personalization of SE in the Mobile Phone by the Patient	No	No	Yes
Personalization of Mobile Healthcare Application (in the Secure Element such as UICC) by Community Cloud of Healthcare (CCH)	No	No	Yes
Multi-Protocol Attack	No	No	Yes
Three-Factor authentication	No	Yes	Yes
Confidentiality	No	Yes	Yes
Two-Factor authentication	Yes	No	Yes
Anonymity of the Patient	Yes	Yes	Yes
Mutual authentication	Yes	Yes	Yes
Session key agreement	Yes	No	Yes
Replay attack	Yes	Yes	Yes
Impersonation attack	Yes	Yes	Yes
Stolen Secure Element attack	Yes	Yes	Yes
Formal Verification using Scyther and BAN Logic	No	No	Yes
Non-Repudiation	No	Yes	Yes
Data Integrity	Yes	Yes	Yes
HIPAA standards are ensured	No	No	Yes
MITM Attack	Yes	Yes	Yes

Yes: Provides the feature; No: Doesn't provide the feature. N.A.: Not Applicable

5. CONCLUSION

This work was motivated from ABI research report that infrastructure related to healthcare are prone to attacks which includes Cloud, IOT Wearable Devices, Mobile Network Operator (MNO) and Secure Element (SE) of the patient. This article proposes a Secure and Anonymous Health (SAH) Monitoring System using Wireless Medical Sensor

Networks (WMSN). SAH overcomes all the flaws in the literature using Community Cloud for Healthcare (CCH) and Community Cloud of Certifying Authority (CCCA). SAH framework ensures all the security properties and withstands all the known attacks.

6. ACKNOWLEDGEMENT

The author would like to thank Deanship of Scientific Research at Majmaah University for supporting this work under Project Number No. 1440-37.

7. REFERENCES

Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., & Kumar, N. (2018). A robust and anonymous patient monitoring system using wireless medical sensor networks. *Future Generation Computer Systems*, 80, 483-495.

M.K. Khan, S. Kumari (2014). An improved user authentication protocol for healthcare services via wireless medical sensor networks. Int. J. Distrib. Sens. Netw.10 (4), 1-10.

D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, S.-S. (2013). Yeo; Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Syst. 21 (1) 49–60.

F. Wu, L. Xu, S. Kumari, X. Li (2015). An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. Multimedia Syst. 1–11 http://dx.doi.org/10.1007/s00526-015-0476-3.

X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, M.K. Khan (2015). A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Secur. Commun. Netw. 9 (15), 2643-2655.

Shaik Shakeel Ahamad, V.N. Sastry, Siba K. Udgata (2014).Secure mobile payment framework based on UICC with formal verification. IJCSE 9(4), 355-370.

C. J. F. Cremers. (2006). Scyther-Semantics and Verification of Security Protocols. Ph.D. Dissertation. Eindhoven University of Technology.

Armando, A. et al. (2005). The AVISPA tool for the automated validation of internet security protocols and applications. In Proceedings of Computer Aided Verification'05 (CAV) (LNCS 3576, pp. 281-285).

Muhammad, S., Furqan, Z. and Guha, R.K. (2006). 'Understanding the intruder through attacks on cryptographic protocols', Proceedings of the 44th ACM Southeast Conference (ACMSE2006), March, pp.667–672.

Abadi, M., Burrows, M., Kaufman, C. and Lampson, B. (1993). Authentication and delegation with smart-cards. Science of Computer Programming, 21(2), 93–113.

Burrows, M., Abadi, M. and Needham, R. (1990). A logic of authentication, ACM Transactions on Computer Systems, 8 (1), 18–36.

L. Xu, F. Wu, (2015). Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care. J. Med. Syst.39 (2), 1–9.

Dr. Mohammed Abdulrahman Alshehri is an Assistant Professor at College of Computer and Information Sciences, Majmaah University Majmaah, Saudi Arabia. His research areas include Computer Networks and applications, Network Security, Cyber Security, with specialization in Information Technology.