A Transaction Security Accountability Protocol for Electronic Health Systems

Chian Techapanupreeda
Faculty of Engineering and Technology, Mahanakorn University of Technology, Thailand
chian@mutacth.com

Ekarat Rattagan
Graduate School of Applied Statistics, National Institute of Development Administration, Thailand
ekarat@as.nida.ac.th

Werasak Kurutach
Faculty of Engineering and Technology, Mahanakorn University of Technology, Thailand
werasak@mut.ac.th

Abstract: *In the last two decades, the term "electronic health (e-health) systems" were extensively mentioned in the healthcare industry with the aim of replacing paper usage and increasing productivity. Unfortunately, these systems are not still widely used by healthcare professionals and patients due to the concerns on security and accountability issues. In this article, we propose an accountability transaction protocol to overcome all security issues for implementing electronic health systems. To validate our proposed protocol, we used both Automated Validation of Internet Security Protocols and Applications (AVISPA) and Scyther as the tools to prove its soundness.*

Keywords: *Accountability, transaction security, electronic health records, personal health records, cryptography, scyther tool, AVISPA.*

Received March 14, 2020; accepted September 12, 2021
https://doi.org/10.34028/iajit/19/3/1

1. Introduction

The term "electronic health systems", shortly as "e-health systems", is a "buzzword" that has been widely discussed in the last two decade [21, 25], but the agreed definition is still not clear. Many researchers defined them differently according to their views in different contexts. Consequently, it leads to the unclear meaning of the term "electronic health record" in the real world. In addition, this unclear concept raises the issues on the security and accountability alongside it. This is one of main obstacles in adopting the systems into a real use in the industry. In order to resolve the problem, in this paper, we firstly clarify the meanings of electronic health, Electronic Health Records (EHRs), and accountability in e-health systems and, then, introduce a new protocol for handling e-health transactions with security and accountability. Two well-known and widely acceptable tools, Automated Validation of Internet Security Protocols and Applications (AVISPA) and Scyther, are employed to prove the security soundness of the protocol. We also analyze its efficiency in comparison with others. The main contribution of our works is as follows.

- We proposed a model and protocol that having solid security and having mutual authentication. Mutual authentication can ensure the accountability of the engaging party. That there can deny their action.
- We provide security analysis and two formal verification tools; Scyther, and AVISPA of the proposed protocol. To indicate that our proposed protocol has necessary security properties as Defines, e.g., confidentiality, integrity, authentication, authorization.
- We provide performance analysis of our proposed protocol in communication cost to establish that our proposed protocol can implement in the real-world application.

This paper is organized as follows. Section 2 provides the background concepts of electronic health, EHRs and accountability. Related works are presented in section 3. The proposed protocol is presented and discussed in section 4. Security and protocol analysis is provided in section 5. Finally, Section 6 concludes this work.

2. Background

In this section, the meanings of accountability and e-health are explained as follows.

2.1. Electronic Health

Up until now, there have been various definitions of electronic health (or e-health). Eysenbach [14] defined e-health as an emerging field of medical, public health and business informatics to improve health care at the local, regional and global levels by using Information and Communication Technology (ICT). They argued that the letter "e" in e-health means not only electronic but also efficiency, enhancing quality, evidence based, empowerment, encouragement, education, enabling, extending, ethics and enquiry, which are called 10 e's. They also suggested that e-health should be easy-to-

use, entertaining, exciting and existing. Della-Mea [13] pointed out that the term e-health is integrated-healthcare-systems properties, possibilities, and consequences that more than the sum of the single-component outcomes. And so, there is nothing new, except for the specific interest in healthcare. In conclusion, the author argued that e-health was just a changed name of telemedicine. Oh *et al*. [26] used three keywords, eHealth, E-health and electronic health, to search databases and dictionaries on the Internet for the definitions of eHealth that were proposed during 1999 to 2002. They concluded that the term of "eHealth" is a tacit understanding of its meaning and generally use. This compendium of proposed definitions may improve communication among the many individuals and organizations that may improve communication between individuals and organizations that use the "eHealth" term. They found that eHealth has many various meanings defined by different authors. However, most of those definitions are involved with information technology, Internet and healthcare field.

2.2. Electronic Health Record (EHR)

The term "electronic health record" has been widely used in many research articles with a variety of definitions as mention above. In 2005, Amatayakul and Lazarus [4] have given the definition of an electronic health record as a patient's health information record that provides health profile and behavior to help healthcare professionals or doctors in making the right decision to cure the patient illness. Seymour *et al*. [28] defined an electronic health record as a patient's health record that is collected, created and stored electronically. While, Roman [27] defined that EHR is created from a patient's health record paper system that can be accessed and used only by the healthcare professionals involved in the patient's health records.

2.3. Accountability

In the area of information systems, there are various meanings of the term "accountability" defined by researchers. For example, Feigenbaum *et al.* [15] defined accountability as referring to an entity that is accountable with respect to a certain policy. If this entity violates accountability, a punishment will be raised. The researchers then gave a definition of the terms traces, principal, outcomes and the utility of accountability to create a formal model. According to Gajanayake *et al.* [16, 19] information accountability concerns the use of information where the user is held liable to explain, justify or answer for its use when so requested by the party to whom the information belongs. Boyd [10] defines responsibility as referring to the duties of individuals and what they are required to do to affect a particular decision, while accountability concerns the consequences that ensue once the decision has been made. Accountability in computer security systems involves confidentiality, integrity, authentication, authorization and nonrepudiation of the transaction by all relevant parties. Many researchers have proposed methods, methodology, protocols and processes to comply with accountability procedures. The details of our proposed approach to accountability are described in section 4.

3. Related Works

Accountability in healthcare has become increasingly important and valuable for Health Care Professionals (HCPs), consumers and patients. For instance, HCPs require the patient's entire health record in order to analyze symptoms and make the correct decisions to cure the patient's illness. In contrast, patients need only disclose some of their information (sufficient to diagnose the illness) to the HCPs. However, this may become an obstacle to the implementation of accountability in healthcare systems. Many researchers have proposed different processes and technical applications for healthcare systems. In this section, we will discuss accountability in e-health records in relation to which processes are accountable, which technical applications are used, and other related work. Based on our Techapanupreeda *et al*. [31, 32] we categorized accountability into three classes: accountability in internet transactions; accountability in public management; and accountability in healthcare systems. In the current research, we will focus only on accountability in healthcare systems. Works related to accountability in healthcare systems are described below.

Mashima and Ahamad [23, 24] proposed a protocol to enhance the accountability of EHRs in a way that can be monitored by the patient. This protocol was designed to meet the goals of accountability updating, accountability usage and the protection of honest entities. The researchers designed the protocol based on the CONECT project and direct projects conducted by the federal health architecture program management office and ONC Office of Interoperability and Standards respectively. The protocol uses hybrid cryptographic operations, namely asymmetric encryption and symmetric encryption, to ensure accountability in the use of patient health records. The authors assumed that the patient authorizes access by medical providers such as hospitals, labs, pharmacies and insurance companies. Furthermore, the patient needs to know that his/her healthcare records will be stored by a trusted third party or repository provided by a healthcare facility. This repository is not assumed to be trustworthy, since it simply provides storage space for encrypted health records, and needs to enforce reasonable control regarding access. However, a Monitoring Agent (MoA) is assumed to be trustworthy, as it does not need to know about or store

the contents of health records; the MoA only needs to know when and how data is used or when a repository is updated.

During the years 2013 and 2014, Gajanayake *et al.* [17] proposed several approaches to information accountability for electronic healthcare systems. The authors stated that "information accountability is an idea concerning the appropriate use and after the fact accountability for intentional misuse of information." They also proposed an Information Accountability Framework (IAF) for e-health systems to overcome the impediments that hinder the sharing of sensitive information in e-health systems. An IAF therefore has three main aspects: social, technological and legal. In terms of the social aspects, the authors focus on how consumers perceive their capabilities, policies and procedures. They investigated the impact of information accountability characteristics by measuring the attitudes of future HCPs and e-health consumers in Australia. To do this, the authors conducted two online surveys: the first gauged the attitudes of future HCPs towards Accountable E-Health (AeH) systems, while the second measured the attitudes of potential e-health consumers towards AeH systems. To investigate the technical aspects, the authors used Digital Rights Management (DRM) by employing Open Digital Rights Management (ODRL) to represent policy-based information. ODRL is used to assign usage policies to HCPs. In this way, consumers can provide default usage policies to their preferred HCPs. The authors believe that the main barrier to AeH systems is the representation and manipulation of usage policies. These authors also found that AeH systems require appropriate legislation to underpin governance and regulatory mechanisms, meaning that penalties would be imposed on those who intentionally misuse consumers' data or violate their privacy. The authors claim that their proposed framework for e-health records, the IAF, is adequate. To prevent unauthorized persons from accessing the patient's health records, we use asymmetric and symmetric encryption in the proposed protocol. However, reader can find more encryption time, throughput and memory usage experimented by Aggarwal *et al.* [1].

4. Proposed Protocol for Electronic Healthcare Systems

In the context of information security, many researchers define accountability as involving confidentiality, authorization, authentication, integrity and nonrepudiation. However, based on our literature reviews, we contend that accountability in any electronic transaction processing needs to allow the traceability of activities of all engaging parties with the measures of information privacy and security in order to create trust. This is a very important issue in information systems where data are sensitive, especially in e-healthcare systems. In this section, we will introduce a protocol for data access with the accountability for e-healthcare systems.

4.1. Accountability Protocol

Our methodology for the proposed protocol is based on a hybrid of cryptographic operation. As discussed in section 3, the patient-centric accountability proposed by Mashima and Ahamad [24] is based on cryptographic operations, while in the work of Gajanayake *et al*. [17] it is based on an information accountability framework that ensures accountability for all involved parties. Figure 1 illustrates how each engaging party interacts with another in a transaction. All activities of a transaction can be described as follows. Whenever C (a hospital, a patient, an insurance company or a technical lab) needs to use P's health record, a request is sent to HCP for pre-authentication and authorization. When HCP receives the request from C, the identity of C is verified first. If it is valid, HCP will forward the request to P for authorization. Otherwise, HCP will send a notification back to C and the transaction ends. After receiving the authorization request, P has to decide whether to authorize it or not and, then, notifies HCP of this decision. If it is authorized, HCP will send a message transaction to HA, where the transaction record is kept in a repository. Otherwise, HCP will send a denial of the request to C and the transaction will end. After receiving the patient's health record from HCP, HA will store it in the repository and send an acknowledgement back to HCP. Then, HCP will send the encrypted patient health record to C. After receiving the health record as requested, C will notify HCP. More details of the protocol are explained in the next section.

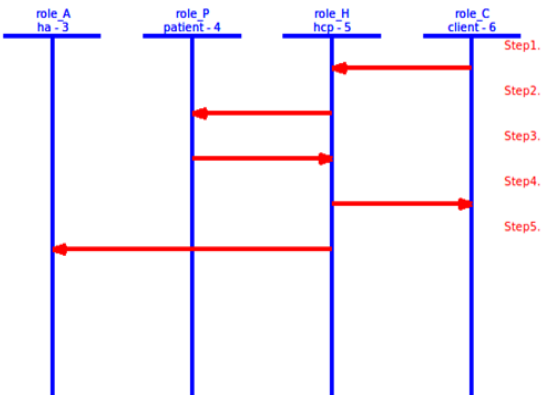

Figure 1. Transaction flow in proposed protocol.

The design of the proposed protocol is based on both asymmetric and symmetric cryptographic operations. The aspects of accountability mentioned in [17] that are confidentiality, integrity, authentication, authorization and nonrepudiation, were considered in designing the protocol. The proposed protocol in [17]

is asymmetric encryption that is not fit for mobile and IoT devices. To meet the requirements for the accountability and privacy of patient health records to use in mobile and IoT environments, we redesigned the protocol to hybrid encryption on both symmetric and asymmetric encryption. The notation used in the proposed protocol is summarized in Table 1.

The previous works about mobile application and IoT devices technique can find more in [2, 7, 8]. Meanwhile, Table 2 shows the steps in the proposed protocol in which messages are sent between parties. If these protocols are not completed before messages are sent to the relevant party, disputes may arise. Therefore, we use security properties such as nonrepudiation to avoid these disputes in the proposed protocol.

Table 1. Notation of the proposed protocol.

Symbol	Definition
P	A patient who owns the personal health records (*PHRs*).
C	Information consumer who needs the PHRs to make a transaction.
HCP	Healthcare professional or clinical the issuer of patient *EHR*s.
HA	Healthcare authority: A service that provides storage for health record transaction. This may be a hospital or a trusted third party.
V	External trusted third party who will verify the transaction if any dispute arises.
P_{ID}	The patient identity or patient number
C_{ID}	The information consumer identity or number
HCP_{ID}	Healthcare professionals/Clinical identity
$Pri\text{-}_Q$	Private key of party Q
$Pub\text{-}_Q$	Public key of party Q
$T_{(i)}$	The system timestamp used as nonce
h(M)	Hash function of message M
$\{M\}_{Pub\text{-}Q}$	Using the public key of Q to encrypt the message M
$\{M\}_{Pri\text{-}Q}$	Using the private key of Q to encrypt the message M
$SK_{A\text{-}B}$	Share key of party A and party B
EHRs/EMRs	An Electronic Health Records/Electronic Medical Records. Inpatient files in hospitals recorded by the healthcare provider.
PHR	Personal Health Records own by individual patient.

Table 2. The proposed protocol.

M1:C→HCP	C_{ID}, P_{ID}, T_1, $\{SK_{C,HCP}\}_{Pub\text{-}HCP}$, $\{h\ (C_{ID}, P_{ID}, T_1)\}_{Pri\text{-}C}$, $\{SK_{C,P}\}_{Pub\text{-}P}$, $h\ (C_{ID}, P_{ID}, T_1, \{h\ (C_{ID}, P_{ID}, T_1)\})_{Pri\text{-}C}$, $(SK_{C,HCP})$, $h\ (C_{ID}, P_{ID}, T_1, \{h\ (C_{ID}, P_{ID}, T_1)\})_{Pri\text{-}C}$, $SK_{C,P}$)
M2: HCP→P	HCP_{ID}, C_{ID}, P_{ID}, T_1, T_2, $\{SK_{HCP,P}, PHR\}_{Pub\text{-}P}$, $\{SK_{C,P}\}_{Pub\text{-}}$, $\{h\ (HCP_{ID,}\ C_{ID}, P_{ID}, PHR, T_1, T_2, SK_{HCP,P})\}_{Pri\text{-}HCP}$, $\{h\ (C_{ID}, P_{ID}, T_1)\}_{Pri\text{-}C}$, $h\ (C_{ID}, P_{ID}, T_1, \{h\ (C_{ID}, P_{ID}, T_1)\}_{Pri\text{-}C}, SK_{C,P})$
M3:P→HCP	$Allow/NotAllow$, $h\ (Allow/NotAllow, HCP_{ID}, C_{ID}, P_{ID}, PHR, T_1, T_2, SK_{P,HCP})$, $h\ (Allow/NotAllow, HCP_{ID}, C_{ID}, P_{ID}, PHR, T_1, T_2, SK_{P,C})$
M4: HCP→HA	$\{h\ (HCP_{ID}, C_{ID}, P_{ID}, T_1, T_2, PHR)\}_{Pri\text{-}HCP}$
M5: HCP→C	T_2, $\{Allow/NotAllow, PHR, T_2\}\ SK_{C,HCP}$, $h\ (\{Allow/NotAllow, PHR, T_2\}\ SK_{C,HCP})$, $h\ (Allow/NotAllow, HCP_{ID}, C_{ID}, P_{ID}, PHR, T_1, T_2, SK_{P,C})$

The details of the proposed protocol are described as follow. Initially, *C* sends a message M1 to *HCP* as a request for permission to access a personal health record of *P*. The message contains the following data: C_{ID}, P_{ID} and timestamp *T1* and the encrypted session key shared between *C* and *HCP*. *HCP's* public key is used for the encryption of the session key to ensure that *HCP* is the only one who is able to open this message. The message M1 also contains the following data:

- $\{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C},\{SK_{C,P}\}_{Pub\text{-}P}$: these data are the hash value of C_{ID}, P_{ID}, *and* T_1 that is encrypted with the private key of *C* and the session key shared between *C* and *P* that is encrypted with the public key of *P*. They are regarded as a message authentication code or token between *C* and *P*.
- $h(C_{ID},P_{ID},T_1,\{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C},(SK_{C,HCP}))$: this data item contains the hash value of C_{ID}, P_{ID}, T_1, the hash value of C_{ID},P_{ID},T_1 that is encrypted with *C's* private key and the session key shared between *C* and *HCP.* It is to ensure that *C* is the sender and *HCP* is the receiver of the message.
- $h(C_{ID},P_{ID},T_1,\{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C},(SK_{C,P}))$: this data item contains the hash value of C_{ID}, P_{ID}, T_1, the hash value of C_{ID},P_{ID},T_1 that is encrypted with *C's* private key and the session key shared between *C* and *P.* It is to ensure that *C* is the sender and *P* is the receiver of the message.

Then, *HCP* sends a message M2 to *P* to request for permission to access *P*'s personal health record. The message contains the following data:

- $HCP_{ID},C_{ID},P_{ID},T_1,T_2,\{SK_{HCP,P},PHR\}_{Pub\text{-}P},\{SK_{C,P}\}_{Pu\ \ P}$: the data includes the session key shared between *HCP* and *P* and the personal health record *PHR* that are encrypted with the public key of *P*.
- $\{h(HCP_{ID,}C_{ID},P_{ID},PHR,T_1,T_2,SK_{HCP,P})\}_{Pri\text{-}HCP}$: this data item is the hash value of $HCP_{ID,}$ C_{ID}, P_{ID}, PHR, T_1, T_2 and the shared key of *HCP* and *P*. By encrypting the hash value with *HCP's* private key, it can authenticates that *HCP* is the sender of the message.
- $\{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C}$: this data item is the encrypted hash value previously received from M1 and then forwarded in M2. It is to ensure that *C* is the requester of the health record.
- $h(C_{ID},P_{ID},T_1,\{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C},SK_{C,P})$: this data item is a hash value previously received from M1 and then forwarded in M2.

After *P* decides whether *C* is allowed to access the health record or not, *P* will inform *HCP* by sending the message M3. The message contains the following data:

- $Allow/NotAllow,h(Allow/NotAllow,HCP_{ID},C_{ID},P_{ID},HR,T_1,T_2,SK_{p,HCP})$: this data item contains the decision result (*Allow/NotAllow*) and the hash value of *Allow/NotAllow*, HCP_{ID}, C_{ID}, P_{ID}, *PHR*, *T1*, *T2* and the session key shared between *P* and *HCP*. The session key is used mainly to ensure the integrity of the message and that *HCP* is the only recipient who

can verify the message.

- $h(Allow/NotAllow,HCP_{ID},C_{ID},P_{ID},PHR,T_1,T_2,SK_{P,C})$: this data item is for communication between *P* and *C*. The session key being hashed with other data is used to ensure the integrity of the message and that *P* is the only recipient who can verify the message.

In the message M4, *HCP* will send the data $\{h(HCP_{ID},C_{ID},P_{ID}, T_1,T_2,PHR)\}_{Pri\text{-}HCP}$ to *HA* to be recorded in the *HA* repository. When a dispute arises between any two parties, the litigant party can request this data item for resolving the problem. That is to say, it contains all the necessary information to use to resolve the dispute.

In the message M5, *HCP* will send the data $T_2,\{Allow/NotAllow,PHR,T_2\}SK_{C,HCP},h(\{Allow/NotAllw, PHR,T_2\}SK_{C,HCP}),h(Allow/NotAllow,HCP_{ID},C_{ID},P_{ID},PH R, T_1,T_2,SK_{P,C})$ to *C*. The objective of this message is to send *P*'s personal health record to *C* as requested with ensuring that *HCP* and *C* are the sender and the receiver of the message, respectively. In addition, by using the shared session key $SK_{C,HCP}$, the receiver, *C*, can verify the integrity of the message. It should be noted that timestamps T_1 and T_2 are used as nonce to protect the replay attack.

5. Security Analysis and Communication Cost of the Proposed Protocol

To analyze the security of the proposed protocol, we address both the privacy and security concerns of patients: the confidentiality and the integrity of *PHRs*, patient authentication, authorization, and nonrepudiation of a transaction between the parties involved. An analysis of the proposed protocol is given below.

5.1. Security Analysis

The proposed protocol uses both symmetric and asymmetric encryptions to ensure that no party can deny the responsibility on generating and sending their own message. Advantages of using asymmetric encryption are that there is no need to exchange shared keys, message authentication and nonrepudiation (in which the user cannot deny sending a message) are ensured, and tampering can be detected if the message is altered by an intruder or hacker. This assumes that the private key of each party is not compromised, and the message is successfully sent to the target receiver.

To analyze the proposed protocol, we formulate the goals of our proposed protocol as follows;

1. All activities and their performers in a transaction can be traced back.
2. An audit trail can ensure the identification of the user and data source and transactions among parties.
3. To overcome the barriers to using *EHR*s in terms of both security and patient privacy, we analyze all aspects of security by using the following proposed protocol.

M1:C→HCP:
$C_{ID},P_{ID},T_1,\{SK_{C,HCP}\}_{Pub\text{-}HCP},\{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C},\{SK_{C,P}\}_{Pub\text{-}P},h(C_{ID},P_{ID},T_1,\{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C},SK_{C,HCP}),h(C_{ID},P_{ID},T_1, \{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C} ,SK_{C,P})$

a) Initially, *C* sends the message M1 to *HCP* to request for *P*'s health records as well as to share the session key with *HCP*. There are several parts of data in M1 which can be described as follows. Firstly, in M1, the consumer's ID, the patient's ID and the timestamp T_1 are sent in plaintexts, but the session key to be shared is encrypted with *HCP*'s public key. Therefore, only *HCP* can read the session key by using its own private key. Secondly, the hash value of *C*'s ID, *P*'s ID and the timestamp T_1 is encrypted with *C*'s private key. This allows *HCP* to be able to verify that *C* is the sender of the message. Thirdly, *C* put $\{SK_{C,P}\}_{Pub\text{-}P}$ into M1 so that *HCP* will forward it to *P*. Since only *P* can read the session key using its own private key, this allows *C* to share the session key with *P*. Fourthly, *C* creates and puts the hash value $h(C_{ID},P_{ID},T1,\{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C},SK_{C,HCP})$ into M1 to send to *HCP*. This allows *HCP* to verify the integrity of the plaintext data in the message M1. Finally, the hash value $h(C_{ID},P_{ID},T_1,\{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C},SK_{C,P})$ in M1 is forwarded to *P* to verify the integrity of the plaintext data.

b) The integrity of the message can be ensured by using the hash function $\{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C}$ encrypted with *C*'s private key. After receiving the hash values of the message from the sender *C*, the receiver (*HCP*) will use *C*'s public key to decrypt the message $\{h(C_{ID},P_{ID},T_1)\}_{Pri\text{-}C}$ and use his/her own private key to decrypt the timestamp T_1. After obtaining the hash value of C_{ID}, P_{ID} and T_1, the *HCP* uses the hash function to get the hash values from the *HCP*'s side. This is used to check whether or not the hash values are equal. If the hash values of the message are equal, the message integrity is satisfied; if not, the receiver can deny the message.

c) The nonrepudiation of transactions means that each party cannot deny their own actions. This is because the message M1 can be used to prove the sender and receiver of the message. If any dispute arises, the relevant party can prove this themselves using the proposed protocol, as described in section 4.

d) Replay attack: the proposed protocol uses timestamps T_1 to T_2 when sending messages over the network. These are unique timestamp values used to protect the system from a replay attack.

e) Man-in-the-middle attack: By using asymmetric cryptography to authenticate transmission and session key share between sender and receiver, an attacker cannot impersonate a relevant party. This

is proved using the Scyther verification tool [29], as shown in Figure 5 and 6.

f) Mutual authentication between parties: mutual authentication of the message is satisfied through the use of *C*'s private key and the *HCP*'s public key. This ensures that *C* is the sender and the *HCP* is the receiver of the message.

g) Patient privacy: we use an encryption technique to hide the patient's personal information and share only the requested information with *C*.

We provide a comparison between the proposed protocol and those developed by [3, 5, 9, 18, 20, 24, 30] in terms of security properties and privacy, as shown in Table 3. It can be seen that the protocol in [24] having all security properties, while that [20] lacks integrity, nonrepudiation, and accountability. Meanwhile, the protocol of [3] lacks privacy, integrity, authorization, nonrepudiation and accountability. Simultaneously, protocol in [5, 9] lack of privacy, nonrepudiation, and accountability. Whereas the protocols in [18, 30] only satisfied in confidentiality, integrity, and authorization. The conclusions of all comparison are shows in Table 3. This can infer that our proposed protocol satisfies all aspects of accountability and privacy.

Table 3. Comparison of the accountability properties and privacy of the proposed protocol.

Security Aspects	[3]	[5]	[9]	[18]	[20]	[24]	[30]	Proposed
Privacy	N	N	N	N	Y	Y	N	Y
Confidentiality	Y	Y	Y	Y	Y	Y	Y	Y
Integrity	N	Y	Y	Y	N	Y	Y	Y
Authentication	Y	W	W	W	W	Y	N	Y
Authorization	N	Y	Y	Y	Y	Y	N	Y
Nonrepudiation	N	N	Y	N	N	Y	Y	Y
Accountability	N	N	Y	N	N	Y	N	Y

*N=No, Y=Yes, W=Weak

5.2. Security Proof

In this subsection, we use the traditional and well-known authentication approach known as the Scyther verification tool [12, 29] AVISPA project [6, 33] and to prove the soundness and security of the proposed protocol.

5.2.1. Authentication Proof based on AVISPA Project

The AVISPA project in the context of Information Society Technologies program funded by the European Union in the Future and Emerging Technologies (FET Open). To proof our proposed protocol, we wrote the simple protocol specification syntax CAS+ language [28] then using the Security Protocol ANimator (SPAN) tool converted to High-Level Protocol Specification Language (HLPSL) to building Message Sequence Charts (MSC). Note that our proposed protocol has encountered all security properties and no attach within bound. The results of On-the-Fly-Model-Checker (OFMC), Attack Searcher (ATSE) and attack simulation are shown in Figures 2, 3, and 4 respectively. More details of SPAN and AVISPA can find in [6, 33].

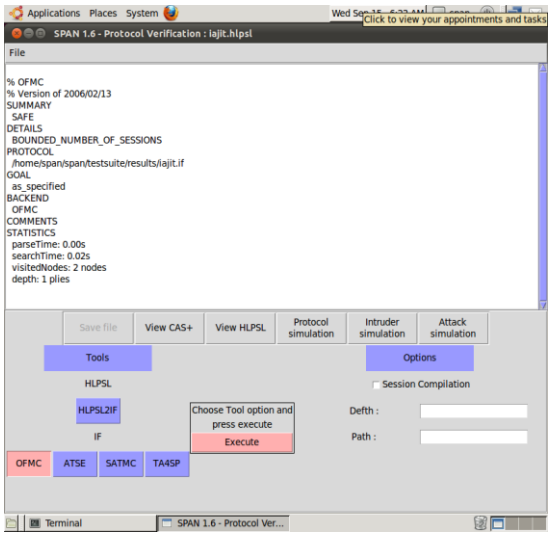

Figure 2. AVISPA OFMC result.

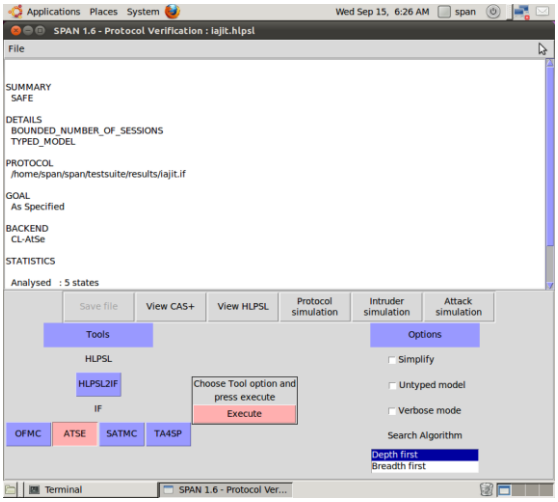

Figure 3. AVISPA ATSE result.

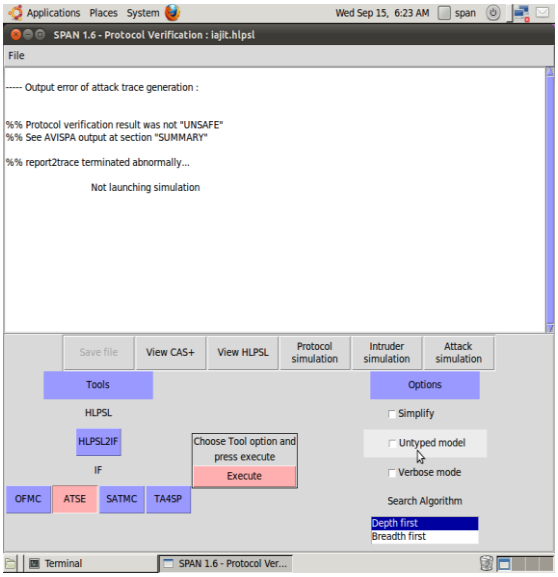

Figure 4. AVISPA attack simulation result.

5.2.2. Authentication Proof based on Scyther Verification

There are many tools for formal verification, as shown in the survey in [29], but the most popular for verification are ProVerif, Scyther and the AVISPA project. These formal verification tools can proof the authentication of the cryptographic protocol. Each of these tools has certain advantages and disadvantages, and the reader can find more information in [29]. The advantage of the Scyther verification tool [12] is its graphical user interface for verification, falsification and analysis of cryptographic protocols.

5.3. Communication Cost comparison

The communication cost is calculated from the transmitted messages size in our proposed protocol and those protocols by [3, 9, 18, 20, 24, 30] the communication cost comparison is show in Figure 5.

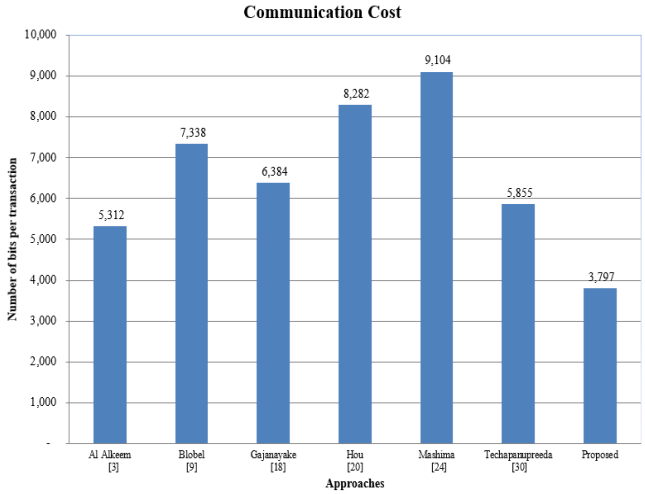

Figure 5. Communication cost comparison.

We therefore used the Scyther verification tool by Security Protocol Description Language (SPDL) to analyze our proposed protocol, as described in section 4. As shown in Figures 6 and 7, the proposed protocol is verified as not attackable. The detail of authentication claim types is explained below.

- Secret: the results show that all parties secret is no attack within bound. Thus, the confidentiality of the data is proved.
- Alive: the output shows aliveness of the transaction of the proposed protocol are available when need.
- Weakagree: the initiator *C* completes a run of the protocol, apparently with responder *HCP*, and then has previously been running the protocol, apparently with.
- Commit: is a specific data agreement e.g., in our proposed protocol *C* agreed with *HCP* on a set of nonce T_1 and T_2.
- Niagree: the proposed protocol achieves a guarantee of non-injective agreement. This can ensure the integrity of the message send between parties.
- Nisynch: the proposed protocol achieves a guarantee of non-injective synchronization to ensure that the protocol has no replay attack and mutual authentication is satisfied [11, 22].

6. Conclusions

In this paper, we propose a protocol for transaction processing in electronic healthcare systems that can achieve our goal in terms of accountability. The novel aspect of this idea lies in the inclusion of certain forms of security that are necessary to protect patient privacy. Firstly, it can ensure that the actions of each party are traceable throughout the movement of data in a transaction. Finally, the protocol meets the requirements of both security and privacy of patient data. Two important tools, AVISPA and Scyther, were employed to prove that our protocol meets the requirement of security properties. In addition, the protocol was analyzed in comparison with other existing protocols.

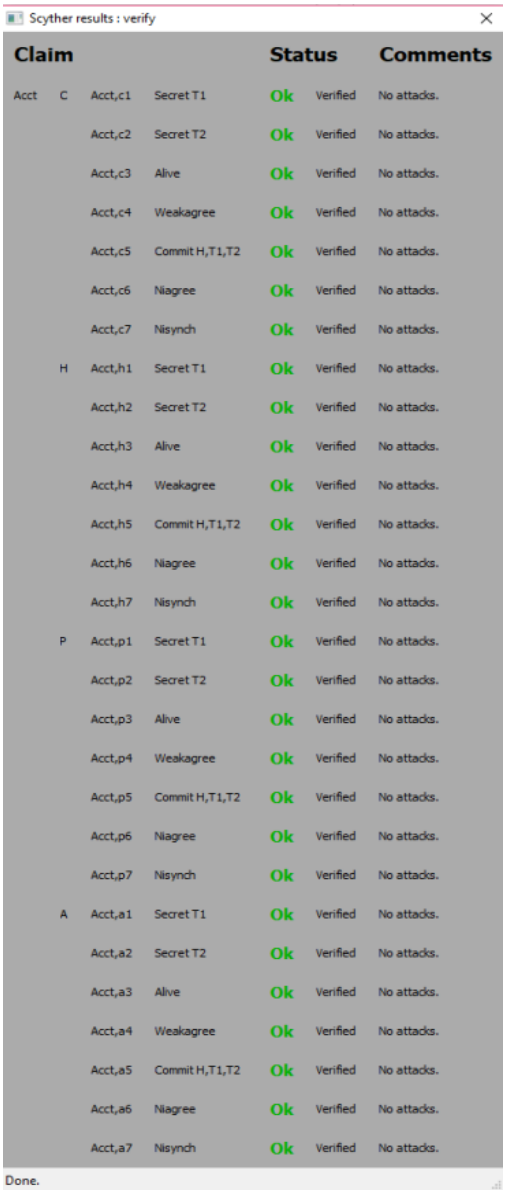

Figure 6. Scyther tool verify claims test for all parties.

Scyther results : autoverify

Claim				Status		Comments
Acct	C	Acct,C1	Secret ni	Ok	Verified	No attacks.
		Acct,C2	Secret nr	Ok	Verified	No attacks.
		Acct,C3	Secret T2	Ok	Verified	No attacks.
		Acct,C4	Secret T1	Ok	Verified	No attacks.
		Acct,C5	Alive	Ok	Verified	No attacks.
		Acct,C6	Weakagree	Ok	Verified	No attacks.
		Acct,C7	Niagree	Ok	Verified	No attacks.
		Acct,C8	Nisynch	Ok	Verified	No attacks.
	H	Acct,H1	Secret T2	Ok	Verified	No attacks.
		Acct,H2	Secret T1	Ok	Verified	No attacks.
		Acct,H3	Secret ni	Ok	Verified	No attacks.
		Acct,H4	Secret nr	Ok	Verified	No attacks.
		Acct,H5	Alive	Ok	Verified	No attacks.
		Acct,H6	Weakagree	Ok	Verified	No attacks.
		Acct,H7	Niagree	Ok	Verified	No attacks.
		Acct,H8	Nisynch	Ok	Verified	No attacks.
	P	Acct,P1	Secret T2	Ok	Verified	No attacks.
		Acct,P2	Secret T1	Ok	Verified	No attacks.
		Acct,P3	Secret ni	Ok	Verified	No attacks.
		Acct,P4	Secret nr	Ok	Verified	No attacks.
		Acct,P5	Alive	Ok	Verified	No attacks.
		Acct,P6	Weakagree	Ok	Verified	No attacks.
		Acct,P7	Niagree	Ok	Verified	No attacks.
		Acct,P8	Nisynch	Ok	Verified	No attacks.
	A	Acct,A1	Secret T2	Ok	Verified	No attacks.
		Acct,A2	Secret T1	Ok	Verified	No attacks.
		Acct,A3	Secret ni	Ok	Verified	No attacks.
		Acct,A4	Secret nr	Ok	Verified	No attacks.
		Acct,A5	Alive	Ok	Verified	No attacks.
		Acct,A6	Weakagree	Ok	Verified	No attacks.
		Acct,A7	Niagree	Ok	Verified	No attacks.
		Acct,A8	Nisynch	Ok	Verified	No attacks.

Done.

Figure 7. Scyther tool auto verity claims test output for all parties.

References

[1] Aggarwal A., Kumar M., and Srivastava A., *Estimation of Various Parameters for AES, DES, and RSA*, Springer Link, 2021.

[2] Aggarwal A., Alshehri M., Kumar M., Alfarraj O., Sharma P., and Pardasani K., "Landslide Data Analysis Using Various Time-Series Forecasting Models," *Computers and Electrical Engineering*, vol. 88, pp. 106858, 2020.

[3] Alkeem E., Shehada D., Yeun C., Zemerly M., and Hu J., "New Secure Healthcare System Using Cloud of Things," *Cluster Computing*, vol. 20, no. 3, pp. 2211-2229, 2017.

[4] Amatayakul M. and Lazarus S., *Electronic Health Records: Transforming your Medical Practice*, Medical Group Management Assn, 2005.

[5] Ameen M., Liu J., and Kwak K., "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications," *Journal of Medical systems*, vol. 36, no. 1, pp. 93-101, 2012.

[6] Armando A., Basin D., Boichut Y., Chevalier Y., Compagna L., Cuéllar J., Drielsma P., Heám P., Kouchnarenko O., Mantovani J., Mödersheim S., Oheimb D., Rusinowitch M., Santiago J., Turuani M., Viganò L., and Vigneron L., "The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications," *in Proceeding of International Conference on Computer Aided Verification*, pp. 281-285, 2005.

[7] Bashir A. and Mir A., "Lightweight Secure MQTT for Mobility Enabled e-health Internet of Things," *The International Arab Journal of Information Technology*, vol. 18, no. 6, pp. 773-781, 2021.

[8] Bhardwaj A., Al-Turjman F., Kumar M., Stephan T., and Mostarda L., "Capturing-The-Invisible (CTI): Behavior-Based Attacks Recognition in Iot-Oriented Industrial Control System," *IEEE Access*, vol. 8, pp. 104956-104966, 2020.

[9] Blobel B., Hoepner P., Joop R., Karnouskos S., Kleinhuis G., and Stassinopoulos G., "Using A Privilege Management Infrastructure for Secure Web-Based E-Health Applications," *Computer Communications*, vol. 26, no. 16, pp. 1863-1872, 2003.

[10] Boyd J., Accountability, pp. 599, McMurry Inc, 2003.

[11] Cremers C. and Mauw S., *Operational Semantics and Verification of Security Protocols*, Springer Link, 2012.

[12] Cremers C., "The Scyther Tool: Verification Falsification and Analysis of Security Protocols," *in Proceeding of International Conference on Computer Aided Verification*, pp. 414-418, 2008.

[13] Della-Mea V., "What is E-Health (2): the Death of Telemedicine?," *Journal of Medical Internet Research*, vol. 3, no. 2, pp. e834, 2001.

[14] Eysenbach G., "What Is E-Health?," *Journal of Medical Internet Research*, vol. 3, no. 2, pp. e20, 2001.

[15] Feigenbaum J., Jaggard A., and Wright R., "Towards a Formal Model of Accountability," *in Proceedings of the New Security Paradigms Workshop*, New York, pp. 45-56, 2011.

[16] Gajanayake R., Iannella R., and Sahama T., "Sharing with Care: An Information Accountability Perspective," *IEEE Internet Computing*, vol. 15, no. 4, pp. 31-38, 2011.

[17] Gajanayake R., Iannella R., and Sahama T., "Privacy by Information Accountability for E-Health Systems," *in Proceedings of 6th International Conference on Industrial and Information Systems*, Kandy, pp. 49-53, 2011.

[18] Gajanayake R., Iannella R., and Sahama T., "Privacy Oriented Access Control For Electronic Health Records," *in Proceedings of Data Usage Management on the Web Workshop at the Worldwide Web Conference*, Germany, pp. 9-16, 2012.

[19] Gajanayake R., Sahama T., Lane B., and Grunwell D., "Designing an Information Accountability Framework for Ehealth," *in Proceedings of IEEE Healthcom 15th International Conference on E-Health Networking, Application and Services*, Lisbon, 2013.

[20] Hou J. and Yeh K., "Novel Authentication Schemes for Iot Based Healthcare Systems," *International Journal of Distributed Sensor Networks*, vol. 11, no. 11, pp. 183659, 2015.

[21] International Telecommunication Union, "Implementing e-Health in Developing Countries: Guidance and Principles," Retrieved, 2008.

[22] Lowe G., "A Hierarchy of Authentication Specifications," *in Proceedings of 10th Computer Security Foundations Workshop*, Rockport, pp. 31-43, 1997.

[23] Mashima D. and Ahamad M., "Enabling Robust Information Accountability in E-Healthcare Systems," *in Proceedings of 3rd USENIX Workshop on Health Security and Privacy*, pp. 1-10, 2012.

[24] Mashima D. and Ahamad M., "Enhancing Accountability of Electronic Health Record Usage via Patient-Centric Monitoring. In HealthSec," *in Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*, Miami, pp. 409-418, 2012.

[25] Mitchell J., *From Telehealth to E-Health: the Unstoppable Rise of E-Health*, Commonwealth Department of Communications, Information Technology and the Arts, 1999.

[26] Oh H., Rizo C., Enkin M., and Jadad A., "What Is Ehealth?: A Systematic Review of Published Definitions," *World Hosp Health Serv*, vol. 41, no. 1, pp. 32-40, 2005.

[27] Roman L., "Combined EMR, EHR and PHR Manage Data for Better Health," *Drug Store News*, vol. 31, no. 9, pp. 40-78, 2009.

[28] Seymour T., Frantsvog D., and Graeber T., "Electronic Health Records (EHR)," *American Journal of Health Sciences*, vol. 3, no. 3, pp. 201-210, 2014.

[29] Shinde A., Umbarkar A., and Pillai N., "Cryptographic Protocols Specification and Verification Tools-A Survey," *ICTACT Journal on Communication Technology*, vol. 8, no. 2, pp. 1533-1539, 2017.

[30] Techapanupreeda C. and Chokngamwong R., "Accountability for Electronic-Health Systems," *in Proceedings of IEEE Region 10 Conference*, Singapore, pp. 2503-2506, 2016.

[31] Techapanupreeda C., Chokngamwong R., Thammarat C., and Kungpisdan S., "An Accountability Model for Internet Transactions," *in Proceedings of Information Networking, International Conference on*, Cambodia, pp. 127-132, 2015.

[32] Techapanupreeda C., Chokngamwong R., Thammarat C., and Kungpisdan S., "Accountability in Internet Transactions Revisited," *in Proceedings of 14th International Symposium on Communications and Information Technologies*, pp. 378-382, 2014.

[33] Viganò L., "Automated Security Protocol Analysis with the AVISPA Tool," *Electronic Notes in Theoretical Computer Scienc*e, vol. 155, pp. 61-86, 2006.

Chian Techapanupreeda received a bachelor's degree in business administration from Saint John University, Thailand, in 1993; and a Master of Science (MS) in Computer Information Management from Assumption University, Thailand, in 1997, and the Ph.D. degree in Information Technology from Mahanakorn University of Technology, Thailand, in 2019. His research interests include cryptography, network security, wireless networks, and mobile computing and applications

Ekarat Rattagan received the Bachelor of Architecture (B.Arch) from Chulalongkorn University, in 1999, the MS degree in Information Technology from King Mongkuts University of Technology Thonburi (KMUTT), Bangkok, Thailand, in 2003, and the Ph.D. degree in Electrical Engineering and Computer Science from National Chiao Tung University, Hsinchu, Taiwan, in 2016. He is currently a lecturer in the Graduate School of Applied Statistics, National Institute of Development Administration, Bangkok, Thailand. His research interests include Data Analytics and Data Sciences.

Werasak Kurutach received a BE (2nd Class Honors) in Electrical Engineering from King Mongkut's Institute of Technology, Ladkrabang, Thailand, in 1985; a ME in Computer Science from Asian Institute of Technology, Thailand, in 1987; and a PhD in Computer Science and Engineering from The University of New South Wales, Australia, in 1995. Currently, he is an Associate Professor in Department of Information Technology, Mahanakorn University of Technology, Thailand. His research interests include data mining, uncertain and temporal data management, image processing and machine learning.