Information Technology and Management (2020) 21:95–114
https://doi.org/10.1007/s10799-019-00306-z

AGE: authentication in gadget-free healthcare environments

Tanesh Kumar[1] · An Braeken[2] · Anca Delia Jurcut[3] · Madhusanka Liyanage[1] · Mika Ylianttila[1]

Published online: 3 October 2019

Abstract
Mobile and sensor related technologies are significantly revolutionizing the medical and healthcare sectors. In current healthcare systems, gadgets are the prominent way of acquiring medical services. However, the recent technological advancements in smart and ambient environments are offering users new ways to access the healthcare services without using any explicit gadgets. One of the key challenges in such gadget-free environments is performing secure user authentication with the intelligent surroundings. For example, a secure, efficient and user-friendly authentication mechanism is essential for elderly/disabled people or patients in critical conditions requiring medical services. Hence, modern authentication systems should be sophisticated enough to identify such patients without requiring their physical efforts or placing gadgets on them. This paper proposes an anonymous and privacy-preserving biometrics based authentication scheme for such gadget-free healthcare environment. We performed formal security verification of our proposed scheme using CDVT /AD tool and our results indicate that the proposed scheme is secure for such smart and gadget-free environments. We verify that the proposed scheme can resist against various well-known security attacks. Moreover, the proposed system showed better performance as compared with existing biometrics based remote user authentication schemes.

Keywords Gadget-free world · Authentication · Smart healthcare · Biometrics · Ambient communication · Internet of Things · Industry 4.0

1 Introduction

The rapid developments and continuous enhancements in technologies such as smart sensing and Internet of Things (IoTs) [62] together with high speed communication technologies, e.g. 5G have strengthened the concept of ambient intelligence [2, 5]. These offer new opportunities and ways in the practical implementation of such smart systems in our daily life for different purposes. Smart sensing technologies and printed electronics are taking us closer to the vision of complete ambient and gadget-free environment where services can be acquired anytime and anywhere. The advent of 5G technologies will play a vital role by providing fast and reliable access of services in such smart environments. The ubiquitous and persuasive computing are also considered as driving forces towards the "always available" services and supporting the vision of the future Industry 4.0 [1, 3, 55]. These intelligent and smart surroundings should be sensitive (understands user habits, emotions), adaptive and at the same time responsive according to the user's need [73]. The surroundings should also be context-aware and must be capable of delivering digital services to the required users.

Currently, the widely used way of acquiring digital services is through gadgets. Gadgets such as smartphones, laptops, Personal Digital Assistants (PDAs) and tablets among others are mainly used by people to get desired services.

✉ Tanesh Kumar
tanesh.kumar@oulu.fi

An Braeken
an.braeken@vub.ac.be

Anca Delia Jurcut
anca.jurcut@ucd.ie

Madhusanka Liyanage
madhusanka.liyanage@oulu.fi

Mika Ylianttila
mika.ylianttila@oulu.fi

[1] Centre for Wireless Communications (CWC), University of Oulu, Oulu, Finland

[2] Industrial Engineering INDI, Vrije Universiteit Brussel VUB, Nijverheidskaai 170, 1070 Brussels, Belgium

[3] School of Computer Science, University College Dublin, Dublin, Ireland

The increasing number of connected devices offers huge potential for data gathering and service businesses. However, there is a clear need for a change from the individual user's point of view where they have more control over their personal data. In addition to that, the current trend is also inclining towards wearable devices such as smart watches, smart clothes and fitness bands to access required services. The next major digital paradigm shift will be user-centric, ambient and gadget-free environment. In the gadget-free vision (also known as Naked World), users do not carry explicit gadgets for services, instead they will have seamless interaction with the intelligent environment for getting digital services [4, 32, 54]. In this gadget-free ambient world, one of the core challenges would be to provide the sufficient level of security and privacy. Most of these smart connected devices will have limited resources in terms of power, memory and computations. Thus lightweight security solutions are needed in the implementation and will heavily be used in future smart systems [57].

Healthcare is one of the prominent application areas which has been highly benefited from this technology shift. New technological advancements are shaping various alternative ways for providing healthcare services to patients and elderly/disabled people in the hospital or remotely from home in more secure and efficient ways. Patients, doctors and administration staff can manage and perform their responsibilities in much improved manner and can monitor user's health both while having face to face treatment with patients or even remotely [92]. Also with the continuous increase in elderly population, it is now crucial to have intelligent environments that provide healthcare and well being services effectively, efficiently and with lesser costs, both home and hospitals [24]. Also persons with disabilities face similar kind of problems and require the corresponding health facilities [26]. However, security and privacy are crucial requirements for such smart IoT based healthcare systems and must be addressed carefully before delivery of such key services to various users [7, 20, 80, 93]. For example, user's authentication is vital in these healthcare system to ensure only valid users should able to access or receive the required services [74, 94].

There are numerous proposals for efficient users authentication for healthcare systems available in the literature [39, 63, 70, 87, 88]. The traditional schemes mainly propose two-factor users authentication [60, 87]. However, due to recent advancements in the area of the IoT based healthcare systems, there requires more stronger and efficient ways of authentication as compared with the traditional solutions. In this context, several three-factor authentication schemes are proposed for the healthcare systems that would utilize any of the user's unique biometrics features [43, 69, 95]. These schemes are mainly dependent on secure utilization of gadgets (mobile or laptops) to fetch the required user's biometrics characteristics along with other details (username, password/PIN etc.). These solutions are very suitable and feasible until the user can able to operate the gadgets and familiar with the respective technologies. However, if we consider the case of elderly or senior citizens and disabled persons, it is relatively harder to user gadgets to allow them to access various medical facilities [6, 37, 53]. Such situations demand more intelligent and secure means of users authentication mechanisms which should be less/no dependent on any explicit gadgets and provide intelligence support from IoT based smart environment.

This leads us to the vision of a smart surroundings where the users can able to access ubiquitously available digital services from the nearby ambient environment and with minimum or no support of gadgets [4, 49]. The key challenge in accessing these medical services in the gadget-free and smart environment is the secure authentication mechanism of the user by service or smart environment [21, 23, 29, 32, 35, 66, 91]. The research community are exploring various potential methods for secure authentication mechanism which are mainly based on biometrics features [30, 31, 38, 77]. The most important characteristics of biometrics keys are that they neither can not easily lost or forgotten and nor can not be guessed easily as compared to low-entropy passwords [36]. Efficient authentication mechanisms using these capabilities embedded in the smart surroundings and with less/no intervention of gadgets are becoming vital in various domains of smart cities vision [10, 11, 33, 76, 86]. Some example where researchers already started to explore the potential of biometrics in smart environments are: smart healthcare, automated monitoring, smart transportation and smart manufacturing etc [27, 48, 72]. However, the focus of this paper is in the domain of smart and gadget-free healthcare environment and we further define the usecase scenario in coming sections.

1.1 Motivation

The old age population is growing rapidly in both developed and developing countries. The choice of many senior citizens to live independently creates necessity to provide them improved and self-caring intelligent living environments. Among other services, healthcare services are vital for them and must be delivered according to the user demand and without any delay. However, most of the current healthcare systems still use traditional password based or smart card based authentication. In the case of emergency, it is hard to follow traditional password based identification mechanisms for a critical patient. Also for the disabled persons, who can not perform much physical activities, it is not very convenient to use a gadget-based systems for their identification. Hence, there is a clear need of smart and intelligent gadget-free environment,

which will be useful to provide easy access to healthcare services for senior citizen/critical patients. However, the user authentication is quite challenging in such gadget free healthcare environment as users will not have any gadgets. Therefore, biometrics based efficient and robust authentication solutions are required for future ambient and gadget-free environments.

1.2 Our contributions

Our Contributions in this paper are discussed as follows:

- We first briefly discussed the concept of future gadget-free hyperconnected environment and defined a problem scenario where patients and elderly people need to be authenticated by nearby hospital surrounding without explicit use of gadgets.
- We proposed an efficient and anonymous biometrics based authentication scheme for the future gadget-free treatment in healthcare environments where patients can be securely authenticated by the smart hospital environment.
- We validate the security properties of the proposed scheme by using formal verification technique (CDVT / AD tool). We also analyzed our proposed scheme using informal security analysis.
- And finally, we compared the communication and computation costs of our scheme with existing available well-known remote user biometrics authentication schemes.

1.3 Organization of paper

The rest of the paper is organized as follows. Section 2 introduces the concept of the gadget-free world. Section 3 highlights the previous work, whereas Sects. 4 and 5 elaborate the problem scenario and preliminary aspects required for the scheme. The proposed authentication scheme is presented in Sect. 6. Section 7 provides the formal and informal security analysis of the scheme whereas Sect. 8 mentions the performance analysis of the proposed scheme. We highlighted the discussion and managerial aspects of this system in Sect. 9 and conclude the paper in Sect. 10.

2 Vision of gadget-free world

The Gadget-Free world (also termed as Naked world) refers to the intelligent surroundings, where users can access digital services without using carry-on gadgets [4, 32, 54]. This approach is based on a user centric vision where environments have to play the leading role for delivering services. Digital services are embedded in the environment by using various smart sensors/devices or printed electronics technologies. The transition from gadget to gadget-free world can be determined through three phases; Bearables, Wearables and Nearables as shown in Fig. 1.

- Bearables refer to hand-held devices such as mobile phones, laptops, tablets which are commonly used to get daily life services. This is the current and most popular way of acquiring services and have been around from several years.
- Wearables are digital devices which are worn by users to acquire required services. These devices may include

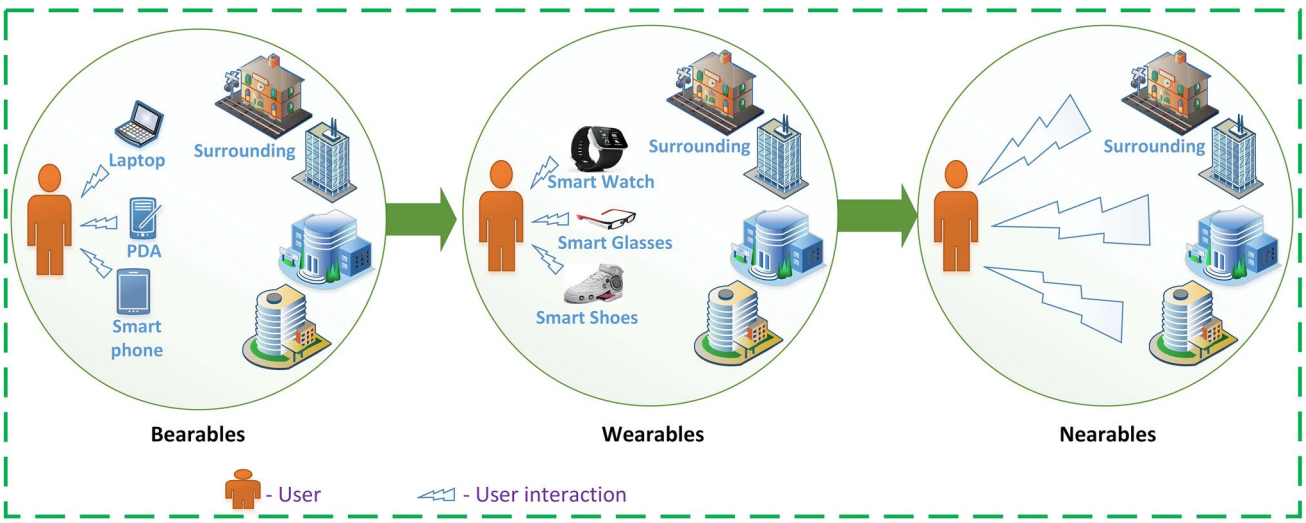

Fig. 1 Transition phases from gadget to gadget-free world

smart watches, smart clothes and fitness bands. From the last decade, the wearable technology is improving and playing a vital role in various applications such as healthcare, military and personal assistance. It is also considered as a useful alternative for hand carry gadgets in some of application areas. IoT and wireless sensor networks technology are providing versatile options to enlarge the scope of wearable devices.

- The last phase towards the gadget-free transition will be Nearables. This phase deals with the direct and seamless interaction of the user with the smart and ambient surrounding where the user does not carry any gadgets or wearables. Almost all the functionalities and services that could be achieved using gadgets or wearables are integrated into nearby environments. Thus, smart sensors/printed electronics along with the required capabilities are embedded within the environment. The interaction of the user will be natural and multi-modal.

The development of transition towards the gadget-free world will require enhancements and evolutions in various communication technologies along with stronger security and privacy solutions. For example, authors in [56] mainly presented the user's privacy challenges in the future gadget-free environments, i.e. data, location and identity privacy. Moreover, considering these privacy challenges, the authors also suggested a conceptual privacy framework that can mitigate these concerns. For example, mechanisms such as access control, anonymity, transparency, data minimization, accountability, and privacy by design among others will be required to ensure the privacy protection in this transition towards gadget-free world. In addition to that, this also requires ethical and legal measures so that each involved stakeholder in such gadget-free digital environment should respect the privacy of others. The work in this article also requires privacy preserving based user authentication in gadget-free healthcare environment and thus privacy characteristics such as identity privacy need to be protected.

The interaction in the gadget-free environment will require different approaches as compared with what we have in the current gadget based interactions. The gadget-free interaction will include multi-modal interfaces and dimensions. Identification mechanisms for the gadget-free world is also among one of the key challenges which need to be addressed. The infrastructure must be capable of identifying authorized users automatically without their own intervention. The identification technologies have also evolved from usernames and passwords to digital user identifiers such as Subscriber Identity Module (SIM) cards or ID tags and then to bio-signatures such as fingerprints, eye scanning, and even DNA. So far, biometrics based identification is considered as the candidate with the highest potential for gadget-free authentication scenarios [32, 54]. Service availability will also drastically change in a future gadget-free environments. The gadget-free world vision allows services to be ubiquitously available and the user can access such services through custom infrastructures. This will open doors for many new applications such as location based applications, positioning and tracking among others which altogether are very critical for the vision of Industry 4.0 applications.

As this gadget-free vision promises that the user still get the required services without carrying gadgets, the means of personal data storage systems would no longer be required. Instead, data is moved from local storages to storages in the infrastructure such as servers or cloud storages. From the gadget-free environment perspective, the data become available for infrastructures embedded systems. The service logic, i.e. applications, is moved from devices to servers. The idea is to make service development and deployment easier, since the number of platforms will be smaller. The gadget-free world will utilize the concepts of edge and fog computing which will push storage and computational capabilities near to the proximity of the user.

3 Related work

In the current digital age, the basic and the most important requirement in many applications is the real-time and reliable authentication of each valid user. Some of the critical applications such as banking transactions, forensics, healthcare and international border security needs stronger, efficient and robust identification. Therefore, the use of biometrics based authentication approaches have rapidly increased over the last decade. The work in [41] presents state of the art in the field of biometrics recognition over the last 50 years including various recent biometrics traits, the potential challenges in biometrics recognition and available solutions corresponding to those issues.

Several symmetric key based smart card two-factor authentication schemes for single-server and multi-server architectures have been described in literature [82]. Several researchers in the past have highlighted the potential vulnerabilities with smart card based two-factor authentication schemes [83]. For example, authors in [9] highlighted that an adversary can follow offline methods to guess the user's password in polynomial time. In addition, there are several threats identified in two-factor authentication for WSN related applications [50, 79]. Authors in [84] explained the potential causes of security failures of two-factor authentication schemes and discussed that researchers only considers attacks on particular protocol and propose corresponding improvements in schemes but pay less focus on underlying rationales of the identified security failures. In order to enhance the security of such schemes further, three factor based authentication schemes

are proposed for multi-server architectures by various researchers where biometrics (e.g. iris, face, retina, fingerprint,) are used as a third factor of authentication [12, 18, 51, 85]. In this work, as we are dealing with gadget-free smart environment for required services and users will be without any hand-carry gadgets, a biometrics based authentication schemes are more suitable option.

Approaches such as fuzzy extractors, fuzzy vaults, and fuzzy commitments are mostly used in the case of the practical integration of biometrics information. They are used to enable the reusability and unlinkability of the proposed system. These techniques use a template and helper data for extracting the secret material [36, 59, 71]. Apart from these approaches, BioHashing technique is also quite useful for similar purposes. It deals with the mapping of the biometrics characteristics randomly onto binary strings with user specific tokenized pseudo-random numbers. Many improved and efficient BioHashing based user authentication mechanisms are presented in the literature that are more feasible for small devices such as smart cards and mobile devices [64, 68]. In this work, we are using the central access point (AP_C) to store the biometrics information of users and thus use of BioHashing can be avoided in this problem scenario.

With the advancement in healthcare technologies, an immense quantity of biomedical sensors will be worn on or implanted in patients in the future for the monitoring, diagnosis, and treatment of diseases. Securing inter-sensor communications within Body Area Networks (BANs) are essential for not only protecting privacy for health related data, but also to guarantee the safety of healthcare delivery. Therefore, biometrics based authentication schemes for BANs are proposed [42, 90]. In addition to that, remote user based telecare medical information systems (TMIS) based healthcare services are getting more widely adopted over traditional desktop telemedicine platforms. Several biometrics based remote user authentication schemes are proposed in the literature to provide protection from certain well-known security attacks such as replay attacks, the Denial of Services (DoS) attacks [17, 40, 78, 81]. Anonymity and unlinkability are also among key requirements for the user while proposing an authentication scheme for smart connected homes, healthcare or for any other critical services [51].

In our problem scenario, we are dealing with direct user's authentication with the environment without using any intervention of a gadget or a device. The work in [54] explains a gadget-free user authentication framework for single user and restricted locations in the hospital environment. The authentication protocol is solely based on the biometrics characteristics as the user does not carry any smart card or gadget on which security material can be entered. This scheme is useful in preserving identity privacy and can also resist various security attacks. In this paper, we enhanced the system used in [54] by expanding for multiple users and locations within a hospital area. Moreover, we increase the adaptability of the system for low power IoT devices by using lightweight operations such as hash and XOR.

4 Problem definition

We consider a potential future ambient healthcare environment where patients come to the hospital to acquire medical services, carrying no explicit gadgets (smartphones, tablets, PDAs). Patients want to access the relevant medical services at any location within the hospital. There are various medical sensors deployed at different regions in the hospital, which are capable of providing medical services to the particular patients. These digital services may consist of monitoring heart beats, pulse rate among other health related measurements. Patients are allowed to go to their respective regions and can acquire services. As the patient carries no explicit gadgets, the camera is placed in the environment used for the identification of the valid patient. This can be achieved by capturing and analyzing biometric characteristics of the patients. The medical sensors need to be activated by a pin code, entered by the patient. The health information, registered by the medical end nodes, can then be sent to the Medical Server (MS), where only the patient is able to access the data. Through dedicated access control mechanisms, this data can further be shared with doctors, staff and close family and friends. However, the last part is not a subject of focus for this paper.

The central administration of the hospital (also called registration center (RC)) is supposed to be a trusted party, which will have access control and generates the required key material for the Access Points (APs) and medical sensors or End Nodes (ENs). The central AP (AP_C) has the capabilities of capturing the biometric features of the patient and can also alert the other APs ($AP_1, AP_2, \ldots AP_n$) within the hospital on the potential arrival of a patient. These APs forward the information further corresponding to their ENs. Considering the resources, especially the APs and ENs are vulnerable to security attacks. Figure 2 represents the system model of the proposed gadget-free healthcare usecase.

5 Preliminary aspects

5.1 Security requirements

Confidentiality Information delivered by the medical sensors can only be derived by the patient, thus not by the RC, the APs, the other ENs, or the MS.

Data authentication Nobody is able to alter the original data. The integrity of the data can be verified by the patient.

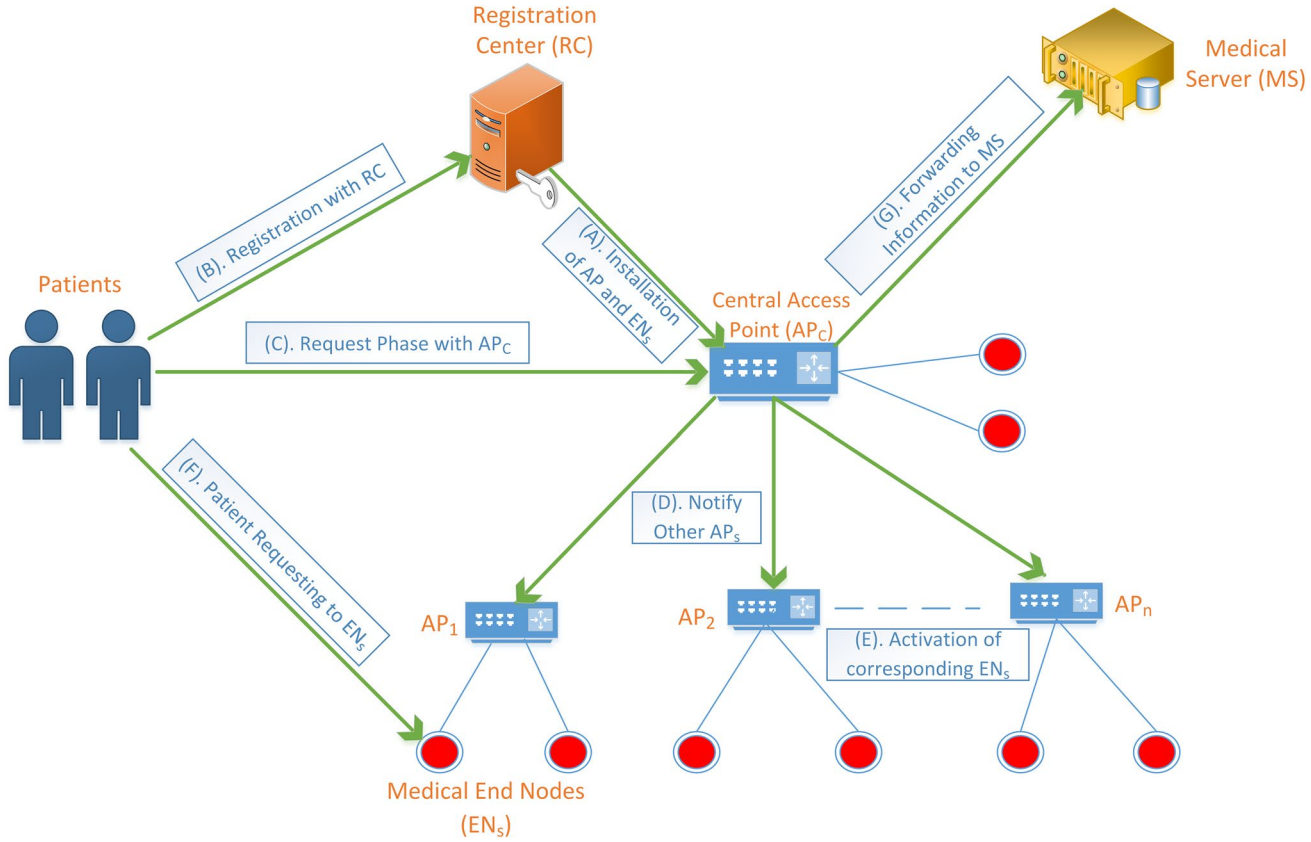

Fig. 2 System model of proposed gadget-free healthcare usecase

Identity privacy It guarantees that the identity of the user cannot be revealed by any outsider.

Unlinkability No outsider is able to link different messages to the same person.

5.2 Setting

In our design, we distinguish five different entities in the system, being the User (U), the Registration Center (RC), the Access Points (APs), the Medical Sensors or End Nodes (ENs) offering health related services and the Medical Server (MS) as shown in Fig. 2. The user in our case is the patient who needs medical services from the ambient and gadget-free environment of the hospital. Patients should not lose their biometric information and should not be traced by different APs.

There are multiple access points available at different regions within the hospital. These access points can be denoted by $(AP_C, AP_1, AP_2, \ldots AP_n)$. The Central Access point (AP_C) is placed at the entrance of the hospital and captures the biometric of each patient that comes to the hospital. All other APs $(AP_1, AP_2, \ldots AP_n)$ are placed at various regions of the hospital. When AP_C captures the biometric details of the patient, it shares the patient related information with the other APs $(AP_1, AP_2, \ldots AP_n)$. These APs are not able to capture biometric information. They can be considered as a gateway between the AP_C and the ENs. The identity related information of the patient, in particular PIN information, should be securely forwarded to the ENs.

The Registration Center (RC) is a trusted party and plays a vital role for the patient's registration. RC is responsible for the generation of key material between the patient and AP_C, the APs and the ENs. End Nodes (EN_S) are responsible for providing medical services and hence they must not derive identity or biometric information of patients and must ensure that whether the particular individual requesting the service is a valid registered patient. The Medical Server (MS) is a central server used to store the patient's medical information and thus only limited people should be able to access the data such as patient, doctors, family members and close friends.

The patient first registers with the *RC* when requesting the services from the *EN* corresponding to a particular *AP*. Then, the *RC* generates the appropriate key material for the central AP (AP_C). After the initialization, the patient can be authenticated by the AP_C. AP_C will further share the patient information with other access points within the hospital such as $(AP_1, AP_2, \ldots AP_n)$. The AP_S will then notify the request

to the associated *ENs*, so that medical end nodes can already be aware about the particular patient and requested service. Next, when the patient is going to utilize the services of a particular EN, it enters its pin code. If this pin code is registered at the EN, the corresponding service can start and the resulting information of the service is then further transmitted through the corresponding AP and the AP_C to the MS.

5.3 Assumptions

We mainly focus on communication between patients and medical end nodes. For the communication between other entities, we assume the existence of secret shared keys. These keys can be established either by physical contact or by a more computer intensive public key infrastructure mechanism. As these techniques are well-known, we do not focus on them in this article. Consequently, the following notations are used for secret shared keys.

- Between registration center and access point: The secret shared key is generated by *RC* and denoted as K_{RCAP_S}. It is used for communication between registration center *RC* and access points *AP*.
- Between end nodes and access points: This key is used between access points AP_S and *EN* and denoted by $K_{AP_SEN_J}$.
- Between registration center and end nodes: The key is generated by *RC* and denoted as K_{RCEN_J}. It is used while sharing information between registration center and end-nodes mainly during installation of end-nodes.
- Between AP_C and other APs: The key is generated by *RC* and denoted as $K_{AP_CAP_S}$. It is used while sharing information from a particular AP to the central AP.
- Between central access point and medical server: The key is denoted by K_{AP_CMS} used while sharing information from central access point to medical server.

An outsider should not be able to derive the identity of the user in the whole process, nor to derive the content of the transmitted data produced by the EN. In addition, even if one of the devices, AP_S or EN_S are tampered, an attacker might not be able to steal the biometric characteristics of the user or to perform other damaging actions. Only authenticated users are able to request services or access to the *ENs*.

The attackers may come from inside or outside the network. They are able to eavesdrop on the traffic, inject new messages, replay and change messages, or spoof other identities. Their goals might be to obtain illegitimate data access to the nodes, to perform service degradation or denial of service.

Table 1 Notation for proposed scheme

Notation	Description
RC	Registration center
AP_S	A particular access point
AP_C	Central access point
MS	Medical server
EN_j	End node j
U_i	User i
x, y	Two secret values by RC
$H(.)$	Hash function
ID_i	Identity of user i
$E_k(.)/D_k(.)$	Symmetric encryption/decryption with key k
BIO_i	Biometrics of user i
PIN_i	Pin code of user i
$\|\|$	Concatenation operator
$\oplus$	XOR operator
T_i	Time stamp
K_{RCAP_S}	Secret shared key between RC and AP_S
$K_{AP_SEN_J}$	Secret shared key between AP_S and EN_J
K_{AP_CMS}	Secret shared key between AP_C and MS
K_{RCEN_J}	Secret shared key between RC and EN_J
$K_{AP_CAP_S}$	Secret shared key between AP_C and AP_S

5.4 Notations

The detailed and frequently used notations in our scheme are mentioned in Table 1.

6 System model

Different phases can be distinguished: (A) the installation phase of ENs and APs (B) registration of the patient with *RC* (C) request phase of patient with AP_C (D) notification of other AP_S (E) activation of the corresponding medical ENs (F) request phase of patient with particular EN_j (G) registration of info and forwarding to the MS. Figure 2 presents the different phases that can be distinguished.

6.1 Installation phase of ENs and APs

Let x, y be two secrets chosen by the *RC*. The identity related information corresponding to a medical end node can be denoted by EN_j. This information is shared using the pre-established secret shared keys K_{RCEN_J} and K_{RCAP_S} respectively.

- ENs: The identity related information EN_j, together with secrets $H(x||y), H(EN_j||H(x))$.
- APs: List of ENs $(EN_1, \ldots, EN_n)$ in its range, together with secret $H(x)$.

6.2 Registration phase

The patient computes a biometric characteristic BIO_i at the time-stamp T_i^1. Next, the patient registers with the RC using BIO_i, ID_i, T_i^1 along with $P_i = H^2(PIN)$.

For each registration, the RC checks the identity of the patient and checks if P_i is not yet available in the database. Next, the following computations are made by the RC. Let N be the number of registrations (counter) for a patient with that identity.

$$A_i = H(y \| ID_i \| N)$$
$$B_i = H(x \| y) \oplus A_i$$
$$D_i = (BIO)_i$$
$$P_i = H^2(PIN_i) \oplus A_i$$

The data $ID_i, N, H^2(PIN_i), T_i^1$ is stored at the RC. The information $H(A_i), B_i, D_i, P_i, T_i^1$ is now securely shared with AP_C, using the secret shared key K_{RCAP_C}.

6.3 Request/login phase of patient with AP_C

Here, when the patient enters in the hospital, AP_C captures the biometric characteristic $(BIO)_i^*$ of the patient and further computes $d(D_i, (BIO)_i^*)$ for all values D_i in the database and checks whether there is a potential candidate, meaning that the distance is lower than the predefined threshold of 0.32 [22]. Note that as shown in [15], if iris recognition is used as biometrics, this threshold equals to 0.32.

Iris recognition is also the best candidate and suggested to be used in our scheme as it has the the smallest percentages of Equal Error Rate (EER), False Accept Rate (FAR) and False Reject Rate (FRR) in comparison with others [13]. Table 2 shows the EER, FAR and FRR of various popular and frequently used biometric traits

6.4 Notification of other APs

Now, the central access point AP_C needs to notify other access points $(AP_1, AP_2, \ldots AP_n)$ present at various locations within the hospital/network, so that they can report to their ENs about the potential arrival of an authenticated patient. Let T_i^2 be the time-stamp at that particular instance, then the group key to be used equals to $K_N = H(H(x) \| T_i^2)$. Consequently, the message $T_i^2, E_{K_N}(H(A_i), B_i, P_i, T_i^2)$ is sent to the other access points $(AP_1, AP_2, \ldots AP_n)$.

Table 2 Accuracy of biometrics computation [13]

Biometric trait (%)	EER (%)	FAR (%)	FRR (%)
Face	NA	1	10
Fingerprint	2	2	2
Hand geometry	1	2	2
Iris	0.01	0.94	0.99
Keystrokes	1.8	7	0.1
Voice	6	2	10

6.5 Activation of corresponding ENs

Next, the access points $(AP_1, AP_2, \ldots AP_n)$ present at various locations within the hospital need to activate their corresponding medical end nodes. Denote a random nonce by N_i. The following computations are made at the AP_S:

$$V_1 = H(EN_j \| H(x)) \oplus N_i$$
$$CID_i = B_i \oplus H(H(EN_j \| H(x)) \| N_i \| T_i^3)$$
$$TK = H(A_i) \oplus N_i$$
$$C_1 = E_{T_K}[P_i \| T_i^3]$$

Here, TK is the temporary key and T_i^3 is the current time-stamp for the set of access points. Next, the AP_S sends the message $V_1 \| CID_i \| C_1 \| T_i^3$ to EN_J. The parameters TK, T_i^3 are added to the memory along with the values $H(A_i), B_i, P_i$.

Upon receiving the message, EN_j executes the following operations using the values stored in the memory.

$$N_i = V_1 \oplus H(EN_j \| H(x))$$
$$B_i = CID_i \oplus H(H(EN_j \| H(x)) \| N_i \| T_i^3)$$
$$A_i = B_i \oplus H(x \| y)$$
$$TK^* = H(A_i) \oplus N_i$$

Next, the decryption of $D_{TK^*}[C_1]$ is done and it is checked whether $T_i^3 = T_i^{3^*}$. Furthermore, information on the pin code is derived by $H^2(PIN_i) = P_i \oplus A_i$. The parameters $H^2(PIN_i)$ and A_i are stored in the memory of the EN_j.

6.6 Request phase patient with EN_j

Suppose the patient wants to use the medical end node EN_j. The patient needs to enter its pin code PIN_i. If $H^2(PIN_i)$ is stored in its memory, the EN_j starts delivering services and recording corresponding information m.

6.7 Registration of info by EN_j and forwarding to MS

Let m be the stream of info, which is generated by the EN_j for the patient, corresponding with the parameters $H^2(PIN_i), A_i$. In order to send m to the MS, such that it can only be read by the authenticated user, which is in the possession of the biometrics and the knowledge of the pin code, it needs to

undergo three communication phases. Denote the current timestamp by T_i^4.

- From EN_j to AP_S:
  Denote $m_{EN} = m \oplus H(H(PIN_i)\|T_i^4)$. Send the following message to the AP_S

  $$T_i^4, T_i^3, E_{TK}(m_{EN}, H(EN_j\|H(PIN_i)\|T_i^4\|m), T_i^4)$$

  If after decryption of the last part of the message by AP_S with the stored TK, the last part corresponds with the first part of the transmitted message, then the AP_S forwards the info to AP_C.
- From AP_S to AP_C:
  The AP_S now sends the message to the AP_C by including identity related information of patient and EN.

  $$T_i^4, H(H(x)\|T_i^4) \oplus AP_S,$$
  $$E_{K_{AP_CAP_S}}(m_{EN}, H(H(EN_j\|H(PIN_i)\|T_i^4)\|m),$$
  $$B_i, EN_j, T_i^4)$$

  If after decryption of the last part of the message by AP_C, the last part corresponds with the first part of the transmitted message, then the AP_C forwards the info to the MS, by including also the biometrics information.
- From AP_C to MS:
  Send the message;
  $T_i^4, E_{K_{AP_CMS}}(m_{EN} \oplus D_i, H(H(EN_j\|H(PIN_i)\|T_i^4)\|m), EN_j, T_i^4)$.

The information $T_i^4, m_{EN} \oplus D_i, H(H(EN_j\|H(PIN_i)\|T_i^4)\|m)$, EN_j is now stored at the MS.Note that we assume that the length of the message m should be shorter than the length of the hash output. If not, instead of using the XOR operation, the message should be encrypted using $H(H(PIN_i), Ti_4)$ as key

If the patient wants to retrieve its information, it first enters PIN_i, Bio_i. From the second part, m can be derived. In addition, the third part allows to verify the integrity of the message.

7 Security analysis of proposed scheme

In this section we present the formal security analysis of our proposed scheme in the gadget-free healthcare environment using Cryptographic-protocol Development and Verification Tools with Attack Detection (CDVT/AD) [46], that is an automated system implementing a modal logic of knowledge [19] and an attack detection theory [47]. Hence, the reason for using CDVT/AD tool to perform the security analysis of our proposed scheme is straightforward; this tool can analyse both: (a) the evolution of knowledge and belief during a protocol execution and therefore it is useful in addressing issues of both security and trust and (b) the design vulnerabilities of a protocol and therefore it is useful for the detection of freshness and interleaving session attacks. Additionally, another benefit of using CDVT/AD tool is that this verification technique is very efficient in terms of memory requirements and execution times (i.e. milliseconds) required for protocol verification [44]. Furthermore, this tool successfully verified a large and various set of security protocols [15, 25, 44].

We formally verify the correctness of our proposed scheme by:

- Formally analyse the security goals of the scheme e.g., authentication, freshness, session-key establishment) using an automated modal logic of knowledge CDVT [19].
- Formally detect any vulnerability in the design of the scheme that may be exploited by freshness or interleaving session attacks [47].

Before looking into these two objectives, we will first explain about CDVT/AD tool itself and message idealization process in the next two sections.

7.1 CDVT/AD tool

The CDVT/AD verification tool uses a parser to read in the protocol specification from a text file. Table 2 summarizes the atomic units of the textual grammar.

Composite data components are constructed according to Table 3, where elements follow the regular expressions as given in Table 2 and "Data" represents an arbitrary data element (either atomic unit or composite data). Statements are defined according to the rules presented in Table 4, where elements follow the regular expressions as given in Table 2,

Table 3 Atomic units of textual grammar

Textual grammar	Textual grammar
Principal	[AB-EIJLMOQRSU-Z] [A-Za-z_0-9_]*
Trusted principal	TTP[A-Za-z0-9_]*
Sym. key	K[a-z][a-zA-Z0-9_]*
Public key	K[a-z][A-Za-z0-9_]*Pub
Private key	K[a-z][A-Za-z0-9_]*Priv
Nonce	N[a-z][A-Za-z0-9_]*
Timestamp	TS[a-z][A-Za-z0-9_]*
Function	F[A-Za-z0-9_]*
Hash	H[A-Za-z0-9_]*
Binary data	[a-z][A-Za-z0-9_]*

Table 4 Composite data construction

Composite data	Textual representation
Concatenation	Data, Data
Group element	(Data)
Symmetric encryption	DataData
Public key encryption	DataKPub
Private key encryption	DataKPriv
Function of data	F(Data)
Hash of data	H(Data)
Key material of data	KMaterial(Data)

"Data" is either an atomic data unit or a composite data as defined in Table 3, "*i*" indicates the indexed discrete time and "Statement" represents an arbitrary statement. "Operator" can be any of: "send", "receive" or "possess", while "Trans_Operator" are the transmission operators and can be any of the following: "send to" or "receive from". The purpose of these transmission operators is to be used for the construction of a specific type of statement expressing reception from a principal or emission to a principal. Each line of the textual specification file is preceded by a label. Assumptions are labeled "An", protocol steps are labeled "Sn" and protocol goals are labeled "Gn", where n numbers each group sequentially. Every line must be closed with a semicolon (';') and comments are introduced by a double forward slash ('//' , C++ style comments).

The inference rules provided are the standard rules of natural deduction. The axioms of the logic of knowledge express the fundamental properties of public-key cryptographic protocols such as the ability of a principal to encrypt/decrypt based on knowledge of a cryptographic key, while the axioms in the case of the attack detection logic theory enable reasoning about message characteristics in cryptographic protocols. The axioms also reflect the underlying assumptions of the logics, which include: (1) The communication environment is reliable, but hostile. That is, message loss or modification can only occur as consequence of hostile intervention; (2)The cryptosystem is ideal. That is, the encryption and decryption functions are completely non-invertible without knowledge of the appropriate cryptographic key and are invertible with knowledge of the appropriate cryptographic key. The cryptosystem is collision-free so that it is not possible to create the same ciphertext from two different pieces of plaintext; (3) A public key used by the system is considered valid if it has not exceeded its validity period and only its rightful owner knows the corresponding secret key; (4) If a piece of data is encrypted/decrypted, then the entity which performed the encryption/decryption must know that data (the data can be plaintext or ciphertext) (Table 5).

Table 5 Statement construction

Principal Operator at[i] Data
Principal $Trans_{O}perator$ Principal at[i] Data
Principal know at[i] Statement
Principal believe at[i] Statement
Principal know at[i] NOT (Statement)
Principal believe at[i] NOT (Statement)
(Statement)
NOT(Statement)
(Statement AND Statement)
(Statement IMPLY Statement)
XOR(Statement, Statement)

7.2 Message idealization

Message idealization is to specify the exchanged messages of the proposed scheme. The following notations are used when translating the scheme into the language of the CDVT/AD tool:

- Registration Center RC: Trusted Third Party TTP;
- Access points of the system APs: Principal Ss;
- Central access point APc: Principal Sc;
- Medical Server MS: Principal Sm;
- End Points ENj: Principal Se;
- Secrets generated by RC x, y: Nx, Ny;
- Hash Function H(.): H();
- IDi (identity of user Ui): U;
- BIOi (bio of Ui): PWbio;
- PINi (Pin of Ui): PWpin;
- ⊕: XOR ;
- Timestamp Ti: Nt;
- Session key between RC and APs Krcaps: Krs;
- Session key between APs and ENj Kapsenj: Kse;
- Session key between APc and MS Kapcms: Kcm;
- Session key between RC and ENj Krcenj: Kre;
- Session key between APc and APs Kapcaps: Kcs;
- Symmetric encryption EK(m): {m}K
- −>: send

The description of the scheme, using the above presented notations is as follows:

7.2.1 Initial phase

- TTP posses: Nx, Ny, Kre, Krx
- Se posses: H(Nx,Ny), H(Se, H(Nx)), Se
- Ss posses: H(Nx), Se

7.2.2 Registration phase

- U posses: PWbio, PWpin, Nt1, U, H(H(PWpin))
- TTP posses: Nn
- expression Ai = H(Ny, U, Nn)
- expression Bi = H(Nx, Ny) XOR Ai = XOR (H(Nx, Ny), H(Ny, U, Nn)) = H(Nx, Ny) H(Ny, U, Nn)
- expression Di = PWbio
- expression Pi = XOR (H(H(PWpin)), H(Ny, U, Nn))
- TTP posses U, Nn, H(H(PWpin)), Nt1, Krc
- Sc posses: H(Ai), Bi, Di, Pi, Nt1, Krc

7.2.3 Request phase of patient with APc

- Sc posses PWbio

7.2.4 Notification of other APs

- Sc , Ss posses Kn = H(H(Nx),Nt2), Nt2
- Sc−>Ss: Nt2, H(H(Ny, U, Nn)), XOR (H(Nx, Ny), H(Ny, U, Nn)), XOR (H(H(PWpin)), H(Ny, U, Nn)), Nt2Kn

7.2.5 Activation of ENj

- expression V1 = XOR (H(IDen, H(Nx)), Ni)
- expression CIDi = XOR (Bi, H(H(EN,H(Nx)),Ni, Nt3))
- expression TK = XOR (H(Ai), Ni)
- expression C1 = Pi, Nt3TK = Pi, Nt3 XOR (H(Ai), Ni)
- Ss−> Se: V1, CIDi, C1, Nt3

7.2.6 Request phase patient with ENj

- U−>Se: PWpin

7.2.7 Registration of info by ENj and forwarding to MS

- Se posses m, Nt4, expression mEN= XOR(H(H(PWpin), Nt4), m)
- Ss−> Sc: Nt4, XOR(H(H(Nx),Nt4),IDaps), mEN, H(H(IDen,H(PWpin),Nt4,m)), Bi, IDen, Nt4 Kcs;
- Sc−> Sm: Nt4, XOR(mEN, Di), H(H(IDen,H(PWpin), Nt4,m)),IDen,Nt4 Kcm;

7.3 Scheme formal proof using the automated CDVT logic of knowledge

Prior to the automated verification using CDVT logic of knowledge, the scheme must be formalized, i.e. translated into the language of the tool. A formalized protocol consists of three components:

- Initial assumptions (conditions that hold before the protocol starts);
- Protocol steps (the messages exchanged between the principals);
- Protocol goals (conditions that are expected to hold if the protocol terminates successfully).

The CDVT/AD tool applies the axioms and rules of the implemented logic of knowledge in an attempt to derive the protocol goals as a logical consequence of the initial assumptions and the protocol steps. If such a derivation exists, the verification is successful and the verified protocol can be considered secure within the scope of the logic.

7.3.1 Formalization of the proposed scheme

Initial assumptions and schemes steps Initial assumptions are statements defining what each principal possesses and knows at the beginning of a protocol run. Figure 3a, b specifies the initial assumptions of the proposed scheme. The proposed scheme steps are formalized in Fig.3c.

Security goals The formalized goals of the scheme are mentioned in Figs. 4 and 5.

7.3.2 Verification results

The results of the automated verification for the above formalized scheme are shown in Fig. 6. As can be seen, all security goals are verified successfully.

7.4 Scheme analysis against design vulnerabilities using CDVT/AD tool

Prior to the automated verification using CDVT/AD for the attack detection [46], the scheme must be formalized into a txt file. The txt file consists of two components: initial assumptions and the protocol steps.

The main idea behind the implemented attack detection technique [47] is to characterize the general circumstances under which a potential attack may exist, by examining the protocol messages structure, and to define a logical formula that describes such circumstances. The logic incorporates detection rules that are classified into five main categories [45] addressing problems related to: (1) message freshness, (2) message symmetries, (3) handshake construction, (4) signed statements and (5) certificates.

The CDVT/AD tool triggers an attack detection rule violation if the prerequisites of the rule can be derived from the formal specification. For any detected failure the analysis will also reveal reasons for the weaknesses, facilitating design corrections. In this case the protocol should be redesigned and re-verified.

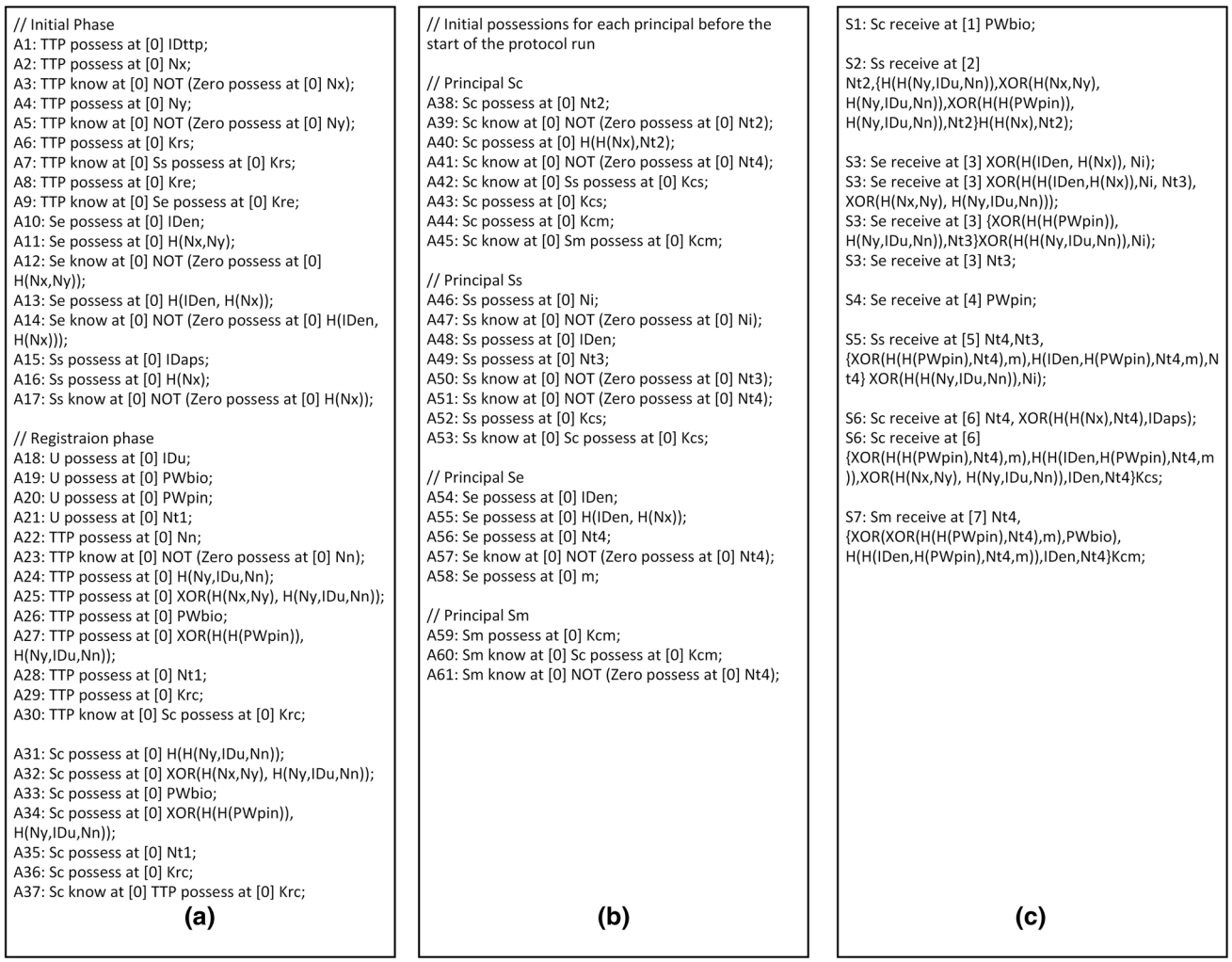

Fig. 3 Scheme formal proof using CDVT/AD: **a**, **b** initial assumptions, **c** scheme steps

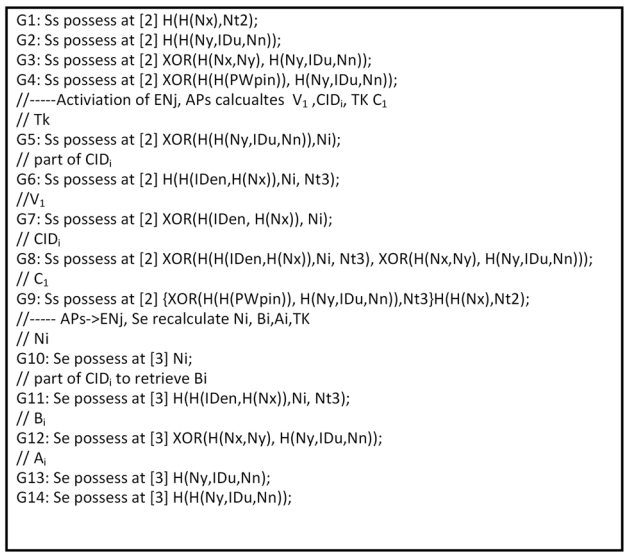

Fig. 4 Security goals (1)

7.4.1 Formalization of the proposed scheme

Initial assumptions Initial assumptions are statements defining what each principal possesses and knows at the beginning of a protocol run. The initial assumptions of the scheme is given in Fig 7a, b. The proposed scheme steps are formalized as shown in Fig. 7c:

7.4.2 Verification results

The results of the verification are shown in Fig. 8. As can be seen, the outcome for the attack detection verification is free of any weakness in the design of the proposed scheme that can be exploited by mountable replay (i.e. freshness) attacks and parallel session (i.e. interleaving session) attacks.

```
// TK
G15: Se possess at [3] XOR(H(H(Ny,IDu,Nn)),Ni);
// Nt3
G16: Se possess at [3] Nt3;
// Pi
G17: Se possess at [3] XOR(H(H(PWpin)), H(Ny,IDu,Nn));
//--------Request phase patient with ENj
G18: Se possess at [3] H(H(PWpin));
//----------Registration of info and forward to MS
//---- ENj -> APs, Se calculate mEN, H(IDen,H(PWpin),Nt4,m)
G19: Se possess at [4] H(H(PWpin),Nt4);
G20: Se possess at [4] XOR(H(H(PWpin),Nt4),m);
G21: Se possess at [4] H(IDen,H(PWpin),Nt4,m);
//---APs re-calculate mEn, H(IDen,H(PWpin),Nt4,m)
// check if APs possess mEn
G22: Ss possess at [5] XOR(H(H(PWpin),Nt4),m);
// check if APs possess H(IDen,H(PWpin),Nt4,m)
G23: Ss possess at [5] H(IDen,H(PWpin),Nt4,m);
// check if APs calculate parameter to Sc
G24: Ss possess at [5] XOR(H(H(Nx),Nt4),IDaps);
G25: Ss possess at [5] H(H(IDen,H(PWpin),Nt4,m));
G26: Sc possess at [6] XOR(H(H(PWpin),Nt4),m);
G27: Sc possess at [6] H(H(IDen,H(PWpin),Nt4,m));
G28: Sc possess at [6] IDen;
G29: Sc possess at [6] XOR(XOR(H(H(PWpin),Nt4),m),PWbio);
//-- APc-> MS
G30: Sm possess at [7] XOR(XOR(H(H(PWpin),Nt4),m),PWbio);
G31: Sm possess at [7] H(H(IDen,H(PWpin),Nt4,m));
//check freshness of information
G32: Se know at [4] NOT (Zero possess at [0]
{XOR(H(H(PWpin),Nt4),m),H(IDen,H(PWpin),Nt4,m),Nt4} XOR(H(H(Ny,IDu,Nn)),Ni));
G33: Ss know at [5] NOT (Zero possess at [0]
{XOR(H(H(PWpin),Nt4),m),H(H(IDen,H(PWpin),Nt4,m)),XOR(H(Nx,Ny),
H(Ny,IDu,Nn)),IDen,Nt4}Kcs);
G34: Sc know at [6] NOT (Zero possess at [0]
{XOR(H(H(PWpin),Nt4),m),H(H(IDen,H(PWpin),Nt4,m)),XOR(H(Nx,Ny),
H(Ny,IDu,Nn)),IDen,Nt4}Kcs);
G35: Sm know at [7] NOT (Zero possess at [0]
{XOR(XOR(H(H(PWpin),Nt4),m),PWbio), H(H(IDen,H(PWpin),Nt4,m)),IDen,Nt4}Kcm);
```

Fig. 5 Security goals (2)

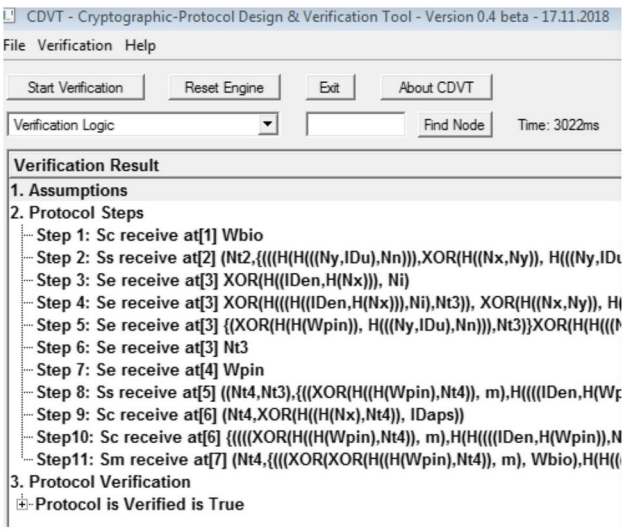

Fig. 6 Security goals verification results

7.5 Discussion on the security features

In this section, we discuss the important security features of the proposed scheme and and its resistance against the most relevant attacks in the literature.

7.5.1 Accountability

Note that a logging mechanism should be installed in each AP and EN. Each log contains identity related information, B_i in case of AP and A_i in case of EN. These parameters give no direct information on a certain identity. However, by keeping track of the same pseudonym, abnormal behavior leading to for instance service degradation and DoS attacks, can be more easily detected. In case of doubt, the RC will be contacted to derive the identity.

7.5.2 Replay attacks

These type of attacks are avoided due to the usage of nonces and timestamps in each communication phase. First at the side of the ENs and APs, since logging is performed, replay attacks will be noticed. Secondly, also the RC keeps track of the number of registrations for a particular identity.

7.5.3 Insider attacks

We distinguish the impact of two different situations, being a compromised AP_S and EN_j.

Compromised AP Let us assume that the attacker has physical access to an AP_S and is able to retrieve the stored information on the device, being a list of valid combinations of $H(A_i), B_i, P_i, T_i^3, TK$, together with the secret value $H(x)$. The attacker will not be able to derive the information delivered by the EN or to create fake information m, as it is not capable to find the value of $H(PIN_i)$.

Compromised end node A compromised end node makes the information P_i, A_i of the patients, together with the stored secret $H(x\|y)$ available. This information cannot be used to find the message m, stored at the MS, since $H(PIN_i)$ is required, which cannot be derived from P_i. However, if a patient uses two times the same pin code, then $H(PIN_i)$ can be registered by the pin code compromised EN and be used to decrypt the stored info at the MS. Consequently, the patient needs to renew its pin code for each usage of the medical EN.

7.5.4 Identity privacy

Note that the activation of the the ENs by the APs contains the parameter CID_i, which is a dynamic reference (nonce is included), related to the pseudonym identity B_i of the patient. Consequently, no outsider can ever link the different requests to a particular user or to the same user. This also guarantees the location privacy of the patient for any outside attacker.

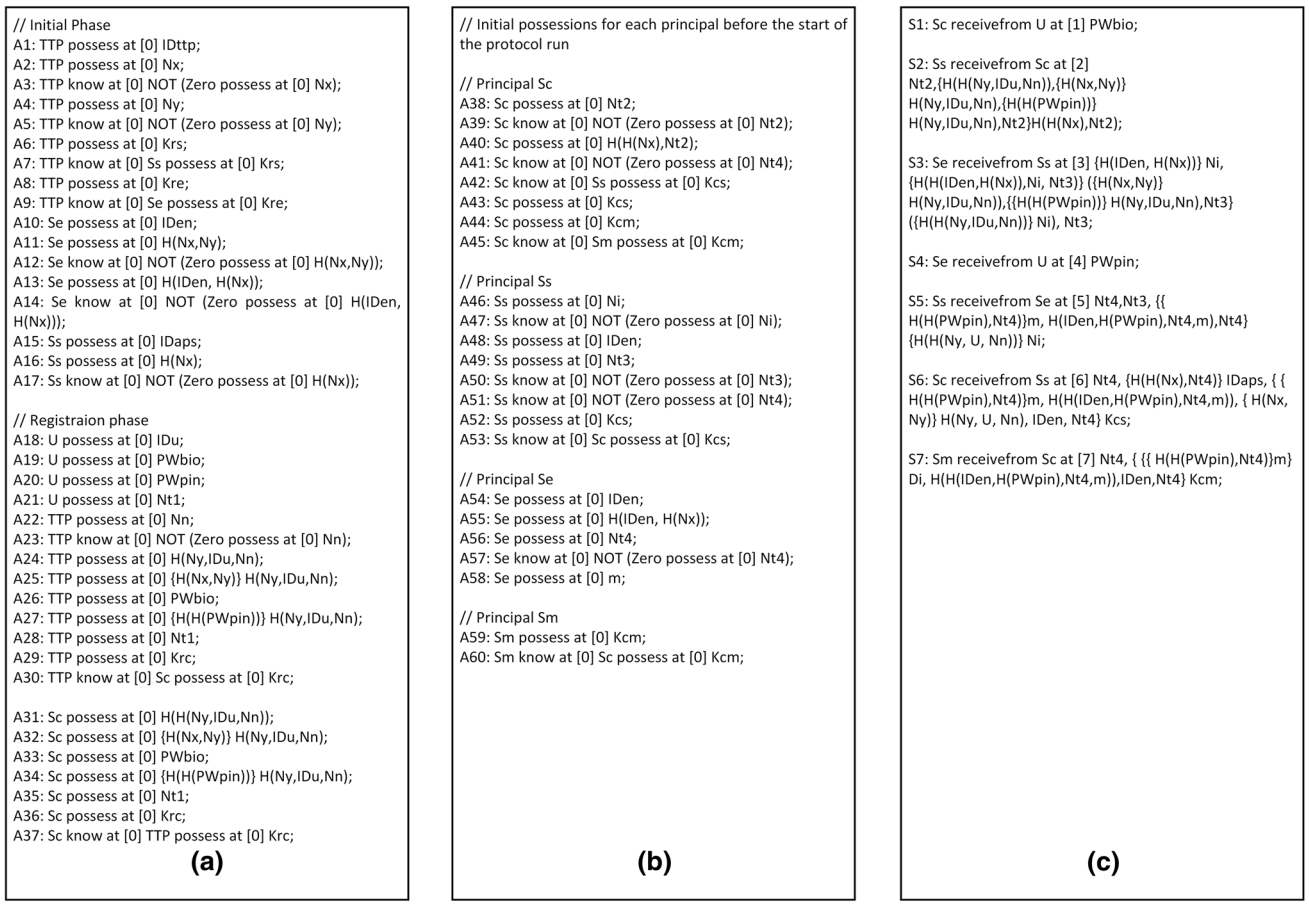

Fig. 7 Analysis of design vulnerabilities using CDVT/AD: **a**, **b** initial assumptions, **c** scheme steps

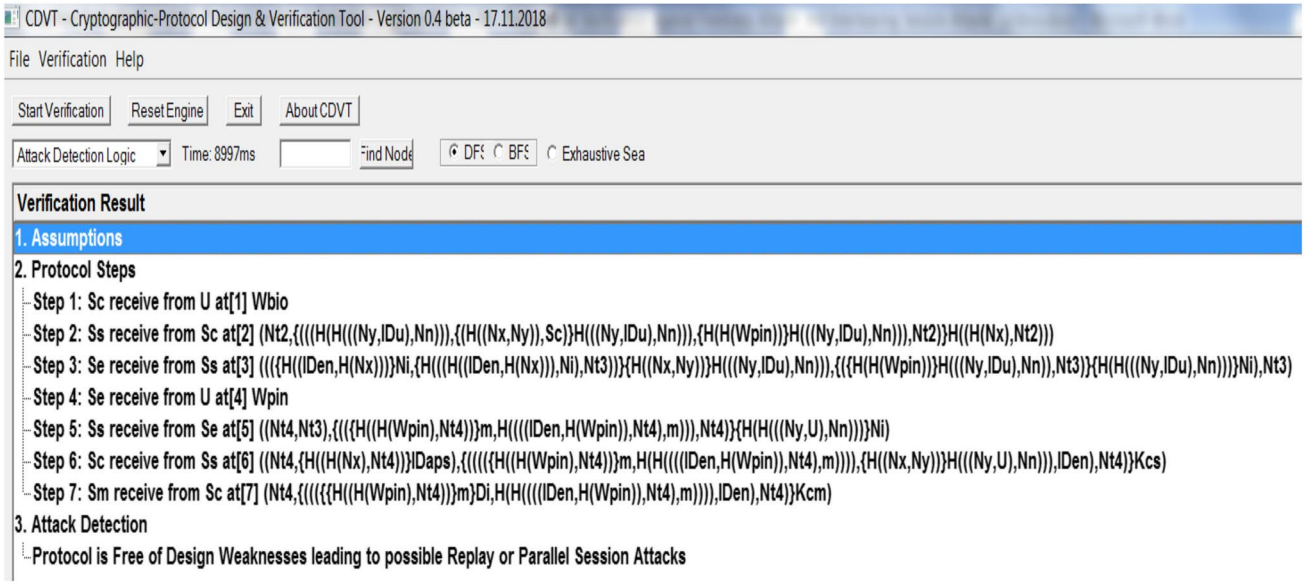

Fig. 8 Attack detection verification results

The same holds for the notification message of the AP_C to the AP_S and the messages in the forwarding phase to the MS. As the identity related information is encrypted using pre-established secret shared keys, it is impossible to link the messages to certain patients.

In all messages to APs and ENs, indirect links $H(A_i)$, B_i with the user's identity are used. Only the RC is able to retrieve the real identity. Note that in contrast to an outsider, the end node does have the possibility to link the requests to the same user. This feature is needed in order to easier detect abnormal behavior.

8 Performance analysis

Here, we analyze the efficiency of the system, being the cost and the accuracy for authenticate a person in order to access the required services. The analysis is split in two parts i.e. the computational cost for cryptographic operations on the authentication protocol and the communication of the messages during the request and response phase.

8.1 Timing for cryptographic/computational operation

In this section, we have computed the computational costs of two major phases in the proposed authentication scheme i.e. the request/login phase and the answer/authentication phase. Suppose T_H represents the time required to execute one way hash function SHA-1, T_S denotes a symmetric key encryption/decryption operation AES and T_M is the time required for an elliptic curve point multiplication [71]. The Elliptic Curve Cryptography (ECC) includes all necessary primitives of asymmetric cryptographic i.e. Elliptic Curve Digital Signature Algorithm (ECDSA), key exchange and agreement protocols. Point multiplication servers are considered as an elementary unit in all ECC and are computationally most complex and expensive operations [8].

We have not included the computational cost for bitwise *XOR* and concatenation because these two operations take relatively very less computational overhead. Based on results presented in [52] , the computation times for T_H, T_S and T_M are 0.0023 ms, 0.0046 ms and 2.226 ms respectively. We have compared results of our biometrics based user authentication directly with smart environments with existing remote biometric authentication schemes (e.g, biometrics based multiserver environments and TMIS). The schemes presented in [16, 17, 34, 36, 40, 40, 58, 61, 71, 75, 78] take higher execution time because of the need for elliptic curve point multiplication and that is not in the case of our proposed scheme as shown in Table 6. The remote biometrics authentication scheme presented in [12] has quite similar computational cost compared with our scheme because it only uses hash functions. Our proposed scheme even slightly performs better than [12], because it uses less number of hash functions and has relatively smaller execution time. As compared with [54], our scheme has slightly higher computation cost because our proposed scheme also contains the forwarding step of medical information from ENs to MS, while scheme in [54] does not cover that.

8.2 Communication cost

We have also calculated the communication costs of the request and answer phases of our proposed scheme and compared it with some of the recent and well-known remote user biometric based schemes. In order to evaluate the communication cost, we used *SHA*-1 as the hash function having 160 bits as the message digest. For the symmetric encryption/decryption, we assume Advanced Encryption Standard (AES) having block sizes of 128 bits. Whereas random nonce and timestamps each take 32 bits. In our scheme during the

Table 6 Comparison of computational cost using our scheme

Scheme	Request	Answer	Total	Total time (ms)
He and Wang [36]	$5T_H + 2T_S + 1T_M$	$12T_H + 4T_S + 7T_M$	$17T_H + 6T_S + 8T_M$	13.417
Baruah et al. [12]	$6T_H$	$7T_H$	$13T_H$	0.0299
Odelu et al. [71]	$4T_H + 2T_S + 1T_M$	$13T_H + 4T_S + 5T_M$	$17T_H + 6T_S + 6T_M$	17.847
Shen et al. [78]	$3T_H + 3T_M$	$14T_H + 3T_M$	$17T_H + 6T_M$	13.395
Chaudhry et al. [17]	$5T_H + 2T_S + 3T_M$	$8T_H + 4T_S + 4T_M$	$13T_H + 6T_S + 7T_M$	15.639
Li et al. [61]	$4T_H + 2T_M$	$16T_H + 4T_M$	$16T_H + 6T_M$	13.402
Kumari et al. [58]	$2T_H + 2T_M$	$14T_H + 6T_M$	$16T_H + 6T_S + 9T_M$	17.840
Chandrakar and Om [16]	$7T_H + 5T_M$	$17T_H + 4T_M$	$24T_H + 9T_M$	20.089
Reddy et al. [75]	$6T_H + 1T_M$	$9T_H + 3T_M$	$15T_H + 4T_M$	28.938
Irshad et al. [40]	$5T_H + 2T_S + 3T_M$	$11T_H + 4T_S + 5T_M$	$16T_H + 6T_S + 8T_M$	18.639
Han et al. [34]	$3T_H + 1T_M$	$8T_H + 1T_M$	$11T_H + 3T_M$	6.703
Kumar et al. [54]	$6T_H$	$5T_H$	$11T_H$	0.0253
Our scheme	$4T_H$	$8T_H$	$12T_H$	0.0276

request phase the message ${T_i}^2, E_{K_N}(H(A_i), B_i, P_i, {T_i}^2)$ requires (32+128) = 160 bits and the message $V_1 \| CID_i \| C_1 \| {T_i}^3$ needs (160+160+128+32) = 480 bits. Hence, the total communication cost at the request phase is (160+480) = 640 bits.

There are multiple messages at answer phase: message $D_{TK^*}[C_1]$ requires 128 bits and forwarding of patient's information from EN to MS requires three messages: T_i^4, T_i^3 ,$E_{TK}(m_{EN}, H(EN_j \| H(PIN_i) \| T_i^4 \| m), T_i^4)$ needs (32+32+128) = 192 bits. Message T_i^4, $H(H(x) \| T_i^4) \oplus AP_S, E_{K_{AP_C AP_S}}(m_{EN}, H(H(EN_j \| H(PIN_i) \| T_i^4) \| m)$, $B_i, EN_j, T_i^4)$ requires (32+160+128) = 320 bits and $T_i^4, E_{K_{AP_C MS}}(m_{EN} \oplus D_i, H(H(EN_j \| H(PIN_i) \| T_i^4) \| m), EN_j, T_i^4)$ needs (32+128) = 160 bits. The total communication cost at answer phase is (128+192+320+160) = 800 bits. Hence as a result, total communication overhead for combined request and answer phases using our proposed scheme is 640+800 = 1440 bits. We can see that our scheme has significantly better communication costs in comparison with [16, 17, 36, 40, 58, 61, 71, 75, 78] which takes 3520 bits, 2944 bits, 2880 bits, 1664 bits, 3360 bits, 3240 bits, 1860 bits, 1440 bits and 1696 bits respectively as shown in Table 7. Though our scheme has little higher communication cost compared with the schemes of [12, 34] and [54] because our scheme takes few more messages for one additional feature such as forwarding the medical information from ENs to MS.

9 Managerial insight and discussion

This gadget-free environment will be crucial in many key applications such as healthcare, smart home, transportation, smart factories and others. This paper mainly deals with the utilization of gadget-free environment in the healthcare sector. The main goal of this paper is to provide a privacy-preserving biometrics based authentication scheme for the treatment of patients in the gadget-free environment. It is important to guarantee that only valid and authorized patients need to authenticate for healthcare services. In future, this gadget-free authentication mechanism can be utilized for other daily life applications in order to verify the valid users. The authentication process may vary from application to application depending upon the security requirements. In a single application/usecase, there might be various layers of authentication required. For example, various gadget-free users in a smart home may have different authentication requirements based on the priority of their requested services.

In the proposed system, each involved entity has to fulfill the assigned responsibility in order to provide secure and gadget-free healthcare services from nearby hospital surroundings. For example, the registration center is a trusted entity in the whole system and thus responsible for sharing the patient's credentials and key material to other entities such as to the access points. Thus, the major managerial responsibilities in the proposed system are carried out by the registration center as a secure entity. Access points are considered as high resourceful devices that can fetch the patient's biometrics and do the further processing with the user's credentials. It is also responsible to send the patient's request to various end nodes available in the hospital environment regarding the desired medical services. End nodes/medical nodes are sensors that have capabilities to verify the valid request from the access point and deliver the basic required healthcare services. The medical server is responsible for storing and processing the patient's data.

The successful patient's authentication in the gadget-free healthcare environment is also crucial for hospital management from various means. For example, the population of old age citizens is increasing worldwide and thus they require basic medical services quite frequently and without doing much physical efforts. This smart and gadget-free healthcare environment will play a key role in delivering such medical services to them. Likewise, such intelligent environments will be helpful for the persons with disabilities. In addition, the traditional healthcare system is using paperwork based patient registration and most of the current healthcare systems use gadget based registration that may take longer and not suitable in the emergencies. Thus, in such emergency situations, these gadget-free healthcare environments are useful for quick registration and can provide fast basic health services. If the hospital management does not adopt such secure gadget-free authentication mechanisms, privacy-based attacks may arise and patient's privacy will be leaked. Furthermore, medical services might get delay or not available in a ubiquitously manner.

Table 7 Comparison of communication cost using our scheme

Scheme	Request (bits)	Answer (bits)	Total cost (bits)
He and Wang [36]	1920	1620	3520
Baruah et al. [12]	640	320	960
Odelu et al. [71]	864	2080	2944
Shen et al. [78]	1920	960	2880
Chaudhry et al. [17]	1152	512	1664
Li et al. [61]	640	2720	3360
Kumari et al. [58]	640	2560	3240
Chandrakar and Om [16]	544	1316	1860
Reddy et al. [75]	800	600	1440
Irshad et al. [40]	832	864	1696
Han et al. [34]	512	704	1216
Kumar et al. [54]	608	448	1052
Our scheme	640	800	1440

This work uses the deterministic based gadget-free environment as we have taken a restricted/limited smart healthcare environment (indoor) along with all defined constraints and variables. The role of each entity has been assigned / mentioned clearly and the output is certainly known. Therefore, deterministic based approaches are appropriate for this proposed indoor/limited healthcare usecase. However, in the future, this gadget-free vision will grow further and would be vital for massive scale smart applications. The transition towards complete deployment of the gadget-free environment will naturally be bounded by the evolution of the required technologies. When the enabling technologies for the complete/outdoor gadget-free environment will become mature, there might be applications where stochastic issues can arise in these intelligent environments due to random factors such as random fluctuation in weather causing unpredicted issues to outdoor gadget-free systems/process. In such cases, various basic optimization approaches can be applied to resolve the issues such as; stochastic gradient descent tricks [14], scenario based stochastic optimizations [67, 89] and cross entropy methods [28] among others [65]. These approaches also vary according to the nature of the application and requirements of that particular usecase in the gadget-free environment.

10 Conclusions

In the present digital era, it is vital that healthcare services should be made readily available in the most natural way possible. Thus, it is crucial to have secure and efficient authentication mechanism for users. In this paper, we have considered the future smart healthcare scenario, where users can acquire digital services without using any hand-held gadgets. We have proposed a secure, efficient and privacy preserving biometrics based authentication mechanism for such intelligent environment solely using lightweight operations. The proposed scheme also achieved anonymity and unlinkability using the lightweight operations and protect the system against the well known security attacks. We have found better results in terms of computation and communication costs for our proposed framework when compared with the previous biometrics schemes. Finally, we also performed the formal security verification of the proposed scheme by using the CDVT/AD tool and examined that our authentication framework is secure for several attacks.

Acknowledgements Open access funding provided by University of Oulu including Oulu University Hospital. This work has been performed under the framework of the Towards Digital Paradise, The Naked Approach, Industrial Edge, the SECURE Connect and 6Genesis Flagship (grant 318927) projects. The authors would also like to acknowledge the contribution of the COST Action CA16226 (SHELD-ON).

References

1. Acampora G, Cook DJ, Rashidi P, Vasilakos AV (2013) A survey on ambient intelligence in healthcare. Proc IEEE 101(12):2470–2494. https://doi.org/10.1109/JPROC.2013.2262913
2. Ahmad I, Kumar T, Liyanage M, Okwuibe J, Ylianttila M, Gurtov A (2017) 5G security: analysis of threats and solutions. In: 2017 IEEE conference on standards for communications and networking (CSCN). IEEE, pp 193–199 (2017)
3. Ahmad I, Kumar T, Liyanage M, Okwuibe J, Ylianttila M, Gurtov A (2018) Overview of 5G security challenges and solutions. IEEE Commun Stand Mag 2(1):36–43
4. Ahmad I, Kumar T, Liyanage M, Ylianttila M, Koskela T, Braysy T, Anttonen A, Pentikinen V, Soininen JP, Huusko J (2018) Towards gadget-free internet services: a roadmap of the naked world. Telemat Inform 35(1):82–92
5. Ahmad I, Shahabuddin S, Kumar T, Okwuibe J, Gurtov A, Ylianttila M (2019) Security for 5G and beyond. IEEE Commun Surv Tutor. https://doi.org/10.1109/COMST.2019.2916180
6. Ahmed E, DeLuca B, Hirowski E, Magee C, Tang I, Coppola JF (2017) Biometrics: password replacement for elderly? In: 2017 IEEE long island systems, applications and technology conference (LISAT). IEEE, pp 1–6
7. Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S (2017) Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egypt Inform J 18(2):113–122
8. Amara M, Siad A (2011) Elliptic curve cryptography and its applications. In: International workshop on systems, signal processing and their applications, WOSSPA, pp 247–250. https://doi.org/10.1109/WOSSPA.2011.5931464
9. Amin R, Islam SH, Biswas G, Khan MK, Leng L, Kumar N (2016) Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. Comput Netw 101(Supplement C):42–62. https://doi.org/10.1016/j.comnet.2016.01.006**(industrial technologies and applications for the Internet of Things)**
10. Ashibani Y, Kauling D, Mahmoud QH (2017) A context-aware authentication framework for smart homes. In: 2017 IEEE 30th Canadian conference on electrical and computer engineering (CCECE). IEEE, pp 1–5
11. Barra S, Castiglione A, De Marsico M, Nappi M, Choo KKR (2018) Cloud-based biometrics (biometrics as a service) for smart cities, nations, and beyond. IEEE Cloud Comput 5(5):92–100
12. Baruah KC, Banerjee S, Dutta MP, Bhunia CT (2015) An improved biometric-based multi-server authentication scheme using smart card. Int J Secur Appl 9(1):397–408
13. Bhattacharyya D, Ranjan R, Alisherov F, Choi M et al (2009) Biometric authentication: a review. Int J u-and e-Service Sci Technol 2(3):13–28

14. Bottou L (2012) Stochastic gradient descent tricks. In: Montavon G, Orr GB, Müller KR (eds) Neural networks: tricks of the trade. Springer, Berlin, pp 421–436
15. Braeken A, Liyanage M, Jurcut AD (2019) Anonymous lightweight proxy based key agreement for IoT (ALPKA). Wirel Person Commun 106(2):345–364
16. Chandrakar P, Om H (2017) A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC. Comput Commun 110:26–34
17. Chaudhry SA, Khan MT, Khan MK, Shon T (2016) A multiserver biometric authentication scheme for tmis using elliptic curve cryptography. J Med Syst 40(11):230
18. Chuang MC, Chen MC (2014) An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Expert Syst Appl 41(4):1411–1418
19. Coffey T, Saidha P (1997) Logic for verifying public-key cryptographic protocols. IEE Proc Comput Digit Tech 144(1):28–32. https://doi.org/10.1049/ip-cdt:19970838
20. Coventry L, Branley D (2018) Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 113:48–52
21. Damopoulos D, Kambourakis G (2019) Hands-free one-time and continuous authentication using glass wearable devices. J Inf Secur Appl 46:138–150
22. Daugman J (2004) How iris recognition works. IEEE Trans Circuits Syst Video Technol 14(1):21–30. https://doi.org/10.1109/TCSVT.2003.818350
23. Dhillon PK, Kalra S (2018) Multi-factor user authentication scheme for IoT-based healthcare services. J Reliab Intell Environ 4(3):141–160
24. Dohr A, Modre-Opsrian R, Drobics M, Hayn D, Schreier G (2010) The internet of things for ambient assisted living. In: 2010 seventh international conference on information technology: new generations, pp 804–809. https://doi.org/10.1109/ITNG.2010.104
25. Dojen R, Chen J, Coffey T (2014) On modelling security protocols for logic-based verification. In: 25th IET Irish signals & systems conference 2014 and 2014 China–Ireland international conference on information and communications technologies (ISSC 2014/CIICT 2014). IEEE
26. Domingo MC (2012) An overview of the internet of things for people with disabilities. J Netw Comput Appl 35(2):584–596. https://doi.org/10.1016/j.jnca.2011.10.015**(simulation and testbeds)**
27. Farrell S (2019) Biometrics in air transport: no flight of fancy. Biom Technol Today 2019(1):5–7
28. Giagkiozis I, Purshouse RC, Fleming PJ (2014) Generalized decomposition and cross entropy methods for many-objective optimization. Inf Sci 282:363–387
29. Grd P, Tomičić I, Baca M (2018) Privacy improvement model for biometric person recognition in ambient intelligence using perceptual hashing. In: Proceedings of the central European cybersecurity conference 2018. ACM, p 18
30. Griffin PH (2015) Security for ambient assisted living: multi-factor authentication in the internet of things. In: 2015 IEEE Globecom workshops (GC Wkshps), pp 1–5. https://doi.org/10.1109/GLOCOMW.2015.7413961
31. Guennouni S, Mansouri A, Ahaitouf A (2019) Biometric systems and their applications. In: Eye tracking and new trends. IntechOpen, pp 1–12
32. Halunen K, Häikiö J, Vallivaara V (2017) Evaluation of user authentication methods in the gadget-free world. Pervasive Mob Comput 40:220–241
33. Hamidi H (2019) An approach to develop the smart health using internet of things and authentication based on biometric technology. Future Gener Comput Syst 91:434–449
34. Han L, Tan X, Wang S, Liang X (2016) An efficient and secure three-factor based authenticated key exchange scheme using elliptic curve cryptosystems. Peer-to-Peer Netw Appl 11(1):63–73
35. Hathaliya JJ, Tanwar S, Tyagi S, Kumar N (2019) Securing electronics healthcare records in healthcare 4.0: a biometric-based approach. Comput Electr Eng 76:398–410
36. He D, Wang D (2015) Robust biometrics-based authentication scheme for multiserver environment. IEEE Syst J 9(3):816–823. https://doi.org/10.1109/JSYST.2014.2301517
37. Helkala K (2012) Disabilities and authentication methods: usability and security. In: 2012 seventh international conference on availability, reliability and security. IEEE, pp 327–334
38. Henniger O, Damer N, Braun A (2017) Opportunities for biometric technologies in smart environments. In: European conference on ambient intelligence. Springer, pp 175–182
39. Hou JL, Yeh KH (2015) Novel authentication schemes for iot based healthcare systems. Int J Distrib Sens Netw 11(11):183,659
40. Irshad A, Sher M, Nawaz O, Chaudhry SA, Khan I, Kumari S (2017) A secure and provable multi-server authenticated key agreement for tmis based on Amin et al. scheme. Multimedia Tools Appl 76(15):16,463–16,489
41. Jain AK, Nandakumar K, Ross A (2016) 50 Years of biometric research: accomplishments, challenges, and opportunities. Pattern Recognit Lett 79(Supplement C):80–105. https://doi.org/10.1016/j.patrec.2015.12.013
42. Jammali N, Fourati LC (2015) PFKA: a physiological feature based key agreement for wireless body area network. In: 2015 international conference on wireless networks and mobile communications (WINCOM). IEEE, pp 1–8
43. Jiang Q, Khan MK, Lu X, Ma J, He D (2016) A privacy preserving three-factor authentication protocol for e-health clouds. J Supercomput 72(10):3826–3849
44. Jurcut A (2018) Automated logic-based technique for formal verification of security protocols. J Adv Comput Netw 6:77–85
45. Jurcut AD, Coffey T, Dojen R (2014) Design guidelines for security protocols to prevent replay & parallel session attacks. Comput Secur 45:255–273
46. Jurcut AD, Coffey T, Dojen R (2014) On the prevention and detection of replay attacks using a logic-based verification tool. In: International conference on computer networks. Springer, pp 128–137
47. Jurcut AD, Coffey T, Dojen R (2017) A novel security protocol attack detection logic with unique fault discovery capability for freshness attacks and interleaving session attacks. IEEE Trans Dependable Secure Comput. https://doi.org/10.1109/TDSC.2017.2725831.
48. Kairinos N (2019) The integration of biometrics and AI. Biom Technol Today 2019(5):8–10
49. Kanagarajan S, Ramakrishnan S (2018) Ubiquitous and ambient intelligence assisted learning environment infrastructures development—a review. Educ Inf Technol 23(1):569–598
50. Khan MK, Alghathbar K (2010) Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'. Sensors 10(3):2450–2459
51. Khan MK, Kumari S (2013) An improved biometrics-based remote user authentication scheme with user anonymity. BioMed Res Int 2013:491289
52. Kilinc HH, Yanik T (2014) A survey of SIP authentication and key agreement schemes. IEEE Commun Surv Tutor 16(2):1005–1023
53. Kowtko MA (2014) Biometric authentication for older adults. In: IEEE long island systems, applications and technology (LISAT) conference 2014. IEEE, pp 1–6

54. Kumar T, Braeken A, Liyanage M, Ylianttila M (2017) Identity privacy preserving biometric based authentication scheme for naked healthcare environment. In: 2017 IEEE international conference on communications (ICC), pp 1–7. https://doi.org/10.1109/ICC.2017.7996966
55. Kumar T, Liyanage M, Ahmad I, Braeken A, Ylianttila M (2018) User privacy, identity and trust in 5G. In: A comprehensive guide to 5G security. Wiley, Hoboken, NJ, USA, pp 267–278
56. Kumar T, Liyanage M, Braeken A, Ahmad I, Ylianttila M (2017) From gadget to gadget-free hyperconnected world: conceptual analysis of user privacy challenges. In: 2017 European conference on networks and communications (EuCNC), pp 1–6. https://doi.org/10.1109/EuCNC.2017.7980650
57. Kumar T, Porambage P, Ahmad I, Liyanage M, Harjula E, Ylianttila M (2018) Securing gadget-free digital services. Computer 51(11):66–77
58. Kumari S, Li X, Wu F, Das AK, Choo KKR, Shen J (2017) Design of a provably secure biometrics-based multi-cloud-server authentication scheme. Future Gener Comput Syst 68:320–330
59. Li P, Yang X, Cao K, Tao X, Wang R, Tian J (2010) An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. J Netw Comput Appl 33(3):207–220. https://doi.org/10.1016/j.jnca.2009.12.003**(recent advances and future directions in biometrics personal identification)**
60. Li X, Niu J, Karuppiah M, Kumari S, Wu F (2016) Secure and efficient two-factor user authentication scheme with user anonymity for network based e-health care applications. J Med Syst 40(12):268
61. Li X, Wang K, Shen J, Kumari S, Wu F, Hu Y (2016) An enhanced biometrics-based user authentication scheme for multi-server environments in critical systems. J Ambient Intell Humaniz Comput 7(3):427–443
62. Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W (2017) A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J 4(5):1125–1142
63. Liu CH, Chung YF (2017) Secure user authentication scheme for wireless healthcare sensor networks. Comput Electr Eng 59:250–261
64. Lu Y, Li L, Peng H, Xie D, Yang Y (2015) Robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. J Med Syst 39(6):65
65. Marinakis Y, Iordanidou GR, Marinaki M (2013) Particle swarm optimization for the vehicle routing problem with stochastic demands. Appl Soft Comput 13(4):1693–1704
66. Matthies DJ, Elvitigala DS, Muthukumarana S, Huber J, Nanayakkara S (2019) CapMat: a smart foot mat for user authentication. In: Proceedings of the 10th augmented human international conference 2019. ACM, p 42
67. Mete HO, Zabinsky ZB (2010) Stochastic optimization of medical supply location and distribution in disaster management. Int J Prod Econ 126(1):76–84
68. Mishra D, Das AK, Mukhopadhyay S (2014) A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. Expert Syst Appl 41(18):8129–8143
69. Mohit P, Amin R, Karati A, Biswas G, Khan MK (2017) A standard mutual authentication protocol for cloud computing based health care system. J Med Syst 41(4):50
70. Moosavi SR, Gia TN, Nigussie E, Rahmani AM, Virtanen S, Tenhunen H, Isoaho J (2016) End-to-end security scheme for mobility enabled healthcare internet of things. Future Gener Comput Syst 64:108–124
71. Odelu V, Das AK, Goswami A (2015) A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Trans Inf Forensics Secur 10(9):1953–1966. https://doi.org/10.1109/TIFS.2015.2439964
72. Orme D (2019) Can biometrics secure the internet of things? Biom Technol Today 2019(5):5–7
73. Palmieri F (2013) Scalable service discovery in ubiquitous and pervasive computing architectures: a percolation-driven approach. Future Gener Comput Syst 29(3):693–703
74. Park Y, Park Y (2017) A selective group authentication scheme for iot-based medical information system. J Med Syst 41(4):48
75. Reddy AG, Yoon EJ, Das AK, Odelu V, Yoo KY (2017) Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment. IEEE Access 5:3622–3639
76. Rose J (2016) Biometrics as a service: the next giant leap? Biom Technol Today 2016(3):7–9
77. Rui Z, Yan Z (2018) A survey on biometric authentication: toward secure and privacy-preserving identification. IEEE Access 7:5994–6009
78. Shen H, Gao C, He D, Wu L (2015) New biometrics-based authentication scheme for multi-server environment in critical systems. J Ambient Intell Humaniz Comput 6(6):825–834
79. Sun DZ, Li JX, Feng ZY, Cao ZF, Xu GQ (2013) On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. Pers Ubiquit Comput 17(5):895–905. https://doi.org/10.1007/s00779-012-0540-3
80. Sun W, Cai Z, Li Y, Liu F, Fang S, Wang G (2018) Security and privacy in the medical internet of things: a review. Secur Commun Netw 2018:5978636
81. Tan Z et al (2013) An efficient biometrics-based authentication scheme for telecare medicine information systems. Network 2(3):200–204
82. Tashi J (2014) Comparative analysis of smart card authentication schemes. IOSR J Comput Eng 16(1):91–97
83. Wang D, He D, Wang P, Chu CH (2015) Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Trans Dependable Secure Comput 12(4):428–442
84. Wang D, Wang P (2014) Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. Ad Hoc Netw 20(Supplement C):1–15. https://doi.org/10.1016/j.adhoc.2014.03.003
85. Wen F, Susilo W, Yang G (2015) Analysis and improvement on a biometric-based remote user authentication scheme using smart cards. Wirel Pers Commun 80(4):1747–1760
86. Wilkins J (2019) Can biometrics secure manufacturing? Biom Technol Today 2019(1):9–11
87. Wu F, Li X, Sangaiah AK, Xu L, Kumari S, Wu L, Shen J (2018) A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Gener Comput Syst 82:727–737
88. Wu F, Xu L, Kumari S, Li X (2017) An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. Multimedia Syst 23(2):195–205
89. Wu L, Shahidehpour M, Li Z (2012) Comparison of scenario-based and interval optimization approaches to stochastic scuc. IEEE Trans Power Syst 27(2):913–921
90. Yao L, Liu B, Wu G, Yao K, Wang J (2011) A biometric key establishment protocol for body area networks. Int J Distrib Sens Netw 7(1):282,986
91. Yeh KH, Su C, Chiu W, Zhou L (2018) I walk, therefore i am: continuous user authentication with plantar biometrics. IEEE Commun Mag 56(2):150–157
92. YIN Y, Zeng Y, Chen X, Fan Y (2016) The internet of things in healthcare: an overview. J Ind Inf Integr 1(Supplement C):3–13. https://doi.org/10.1016/j.jii.2016.03.004

93. Yüksel B, Küpçü A, Özkasap Ö (2017) Research issues for privacy and security of electronic health services. Future Gener Comput Syst 68:1–13
94. Zhang K, Yang K, Liang X, Su Z, Shen X, Luo HH (2015) Security and privacy for mobile healthcare networks: from a quality of protection perspective. IEEE Wirel Commun 22(4):104–112
95. Zhang L, Zhang Y, Tang S, Luo H (2017) Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement. IEEE Trans Ind Electron 65(3):2795–2805