Identity Privacy Preserving Biometric Based Authentication Scheme for Naked Healthcare Environment

Tanesh Kumar[1], An Braeken[2], Madhusanka Liyanage[1], Mika Ylianttila[1]
[1] Centre for Wireless Communications (CWC), University of Oulu, Finland
[2] Industrial Engineering INDI, Vrije Universiteit Brussel VUB, Nijverheidskaai 170, 1070 Brussel
Email: [1]tanesh.kumar@oulu.fi, [2]an.braeken@vub.ac.be, [1]madhusanka.liyanage@oulu.fi, [1]mika.ylianttila@oulu.fi

***Abstract*—Recent developments in Internet of Things (IoT) technologies have already put a huge impact on the medical and health sector. Thus, the patient treatment can be performed in more efficient ways compared with traditional methods. Secure identification is a key system requirement for patients to acquire these health related services. Fast and convenient identification is important in the case of critical and elderly or disabled patients who required frequent health services. In this paper, we are presenting concept of the Naked environment where patients can get health services from smart and intelligent surroundings of hospital without using explicit gadgets. Patients would have direct interaction with the environment and get identified through it. We propose a biometric based authentication scheme for the Naked hospital environment that also protects the patients identity privacy. In addition, we show that this authentication scheme can resist various well known attacks such as insider attacks, replay attacks and identity privacy among others.**

***Index Terms*—Biometrics, Authentication, Security, Naked Environment, Identity Privacy, Internet of Things (IoT), Ambient Assisted Living (AAL)**

I. Introduction

The world is facing a new digital paradigm shift due to recent developments in IoT and wireless sensor networks. These technologies provide useful applications in various areas of daily life, especially in the health care and enhancing well being of people. It facilitates doctors and hospital staff to have continuous monitoring of the health situation of patients. As the population of elderly and senior citizens is increasing steadily along with their choice of living independent, it becomes necessary to have a secure and smart environment where they can be automatically identified from the surrounding and receive services accordingly.

The current world mainly revolves around gadgets, making the user dependent on hand held devices for accessing required services. These gadgets include smartphones, laptops, tablets, Personal Digital Assistant (PDAs) among others. All these digital devices have a proper display for user interaction. Though considering the current trend, wearable technology is somewhat ahead compared with gadgets and they are constantly improving in terms of services. The next major transition is the direct interaction of users with the environment without any help of external gadgets, also known as Naked World [1] [2]. These novel technologies give consumers an immense amount of new services and provide companies new ways for generating revenue. However, security and privacy would always remain the biggest concern, thus it is important to provide secure solutions. As these devices are also resource constrained, lightweight security solutions are needed during the implementation.

The important challenge in this Naked environment is the identification of a valid user. Traditional password based authentication mechanisms might not be suitable and efficient in this case. The usage of biometrics seem to be a potential candidate for identification and authentication in such Naked environment. The uniqueness property of biometrics increases its applications in authentication protocols. The most important characteristics of biometric keys are as follows [3].

- Biometric keys can not be lost or forgotten by the user.
- Biometric keys are extremely hard to forge or distribute.
- Biometric keys are extremely difficult to copy or share.
- Biometric keys can not be guessed easily as compared to low-entropy passwords.
- Someone's biometrics are more difficult to break.

Motivation:

With the advancement in recent communication technologies, there is a clear need for enhancement in living environments for elderly and disabled persons. It is vital to have novel ways of multi-modal interaction and identification of the user with the environment for improved and easy access to services. Health care services are considered crucial for senior people and thus they need to be delivered on time. Therefore, it is required that the environment should be intelligent enough to identify the valid patients and provide digital services accordingly without any external intervention of a third person or device. This would make the identification process faster and reduce the overhead of checking/filling of registration forms. It is also essential in emergency situations in the hospital where critical patients do not have much time and cannot do physical efforts to register themselves. Hence biometrics based efficient authentication solution is needed for smart and ambient environments

Our Contributions and Organization of Paper:

In this paper, we propose an anonymous and biometrics based authentication scheme for the Naked hospital environment. We

consider a hospital scenario and show how patients can get authenticated without using gadgets to access services from their environment. Medical sensors embedded in the environment will provide them the required digital services after secure authentication. Moreover, our proposed scheme can resist various well known attacks such as insider attack, replay attack and identity privacy attack. We have also compared our scheme with some of the already available remote biometric authentication schemes in terms of computational and communication costs.

The rest of the paper is organized as follows. Section II highlights related work on biometrics based identification mechanism. Section III introduces the concept of the Naked World. Sections IV and V explain the problem scenario and preliminary aspects required for the scheme. Section VI elaborates the proposed biometric based authentication scheme. Sections VII and VIII provide the security and performance analysis respectively of the proposed scheme. Finally, we conclude the paper in Section IX.

II. Related Work

Many symmetric key schemes for smart card based authentication on single-server and multi-server architectures have been proposed in literature [4]. Besides smart card based authentication, three-factor based authentication schemes, that even include biometrics, are presented in literature [5-12]. However, as the integration of the biometric information is assumed to be a fixed string (only considered from a theoretical point) and done at the same level as the password introduction, these smart card based protocols can be easily transformed into a biometrics smart card based solution and the other way around. As shown in [5] and [8], most of the proposed smart card based and biometrics based authentication protocols are insecure for well-known attacks like e.g. stolen smart card attacks, replay attacks, user impersonation attacks, and insider attacks. In [13], a new secure system based on ideas of [5] is proposed that offers in addition identity privacy and untraceability. On the other hand, for the practical integration of biometric information, fuzzy extractors, fuzzy vaults, and fuzzy commitments are mostly applied to enable reusability and unlinkability. These techniques use a template and helper data for extracting the secret material. Unfortunately, all these mechanisms require high complexity and a serious performance cost [3, 14, 15]. In [16], the usage of a Pseudo Random Number Generator (PRNG) is proposed for the derivation of a secure and computationally efficient remote biometric authentication scheme, providing a new mechanism for adding strong biometric data protection to a wide range of existing available authentication protocols. The scheme in [17] is called a blind biometric authentication protocol since it ensures the template protection and the user's privacy. The protocol is blind because it shows no other information of the user except his/her identity. It also makes use of a PRNG on server side.

For our Naked World scenario, we need to combine the approaches of server authentication with the practical integration of biometric information into the schemes. To this purpose, we adapt the system of [13] in order to base the authentication solely on the biometric characteristics as the user does not carry any smart card or gadget on which the security material can be entered. To include the biometric information in a performant way into the system, we propose a masking operation with the output of a PRNG.

III. Vision of Naked World

The concept of the Naked World refers mainly to the user centric approach where the user does not need to interact with gadgets or wearables in order to access the digital services [1] [2]. Services are embedded within the intelligent environment through some sensors and they will be available when required and disappear when not needed. The transition from gadget to the Naked World can easily be defined by three key phases i.e. bearable, wearable and nearable.

- Bearables are kind of hand held gadgets which are the most common way of acquiring digital services nowadays. The most commonly used bearables are smartphones, laptops, tablets and PDAs.
- The current trend of bearables are getting declined due to wearable technology. Wearables are digital devices, which are worn by users to get digital services. It is the combination of smart sensors along with fashionable wearing items to have stylish wearable devices. Some of the most used wearables are smart watches, smart clothes and google glasses among others. Wearables have a huge application in healthcare because nowadays it is used frequently to monitor the fitness and health parameters of users like heart rate, temperature and blood pressure.
- Nearables are the final phase towards the Naked World where the user would have direct and seamless interaction with the smart surrounding. The digital services appear to the user from the texture of the environment when needed.

During the transition from gadget to the Naked World, there are a number of factors that are need to evolve. For instance, the interaction of the user will be quite different from the current gadget based interaction. Multi-modal interfaces will be required for the user's seamless interaction with the environment. The data sharing is another major thing which would also change as we move from gadget centric to the user centric world. The data is collected and shared by the environment, devices and systems present in the environment. The data is moved from local storages to storages in the infrastructure, such as servers or clouds. The identification of the user would also be different from the current username and password based solutions. The biometrics based identification mechanisms seem to be an ideal candidate for the Naked environment, but require special attention with respect to theft and tamper resistance.

IV. Problem Scenario

We consider a potential hospital scenario, where an elderly person or critical patient can directly be authenticated by the smart environment in order to avail the required health care facilities as shown in Figure 1. These services may include the monitoring of the pulse rate, the blood pressure and heart

beats of patients. The medical sensors are embedded in the environment to provide the services. We assume that when a patient enters a room in the hospital, he/she does not carry any gadget for the identification, instead the camera/device placed in the environment can directly authenticate him/her. Biometric features are used for the authentication of the patient in this Naked environment. If the results of these services are presented to the patient on a screen or device present in the room, we need to assume that at a single time only one patient is available in the room (no other patient at one time, i.e. doctors or nurses may be in the room) in order to ensure the confidentiality of the information. On the other hand, if the information retrieved by the services is consulted afterwards by the patient by logging into a secure platform, this restriction can drop.

The central administration of the hospital (also called the registration center) is supposed to be a trusted party, which will have access control and generate the required key material for the Access Point (AP). The AP has capabilities to capture the biometric features of the patient and can retrieve the required services of the user from the remote sensors, that is then sent to the medical server. This server contains all the medical information about patients. In particular the AP and the remote sensors are vulnerable to security attacks.

V. Preliminary aspects

A. Security Requirements

Confidentiality: Information of the patient is kept secret from all unauthorized entities available in the surrounding.

Data Authentication: Any authorized person should not be able to alter the original data.

Access Control: The access of the data should be controlled by the central administration of the hospital and no other entity should be able to access it.

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

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

B. Setting

We distinguish four different entities in the system, being the User (U), the Registration Center (RC), the Access Point (AP), and the Sensors or End Nodes (ENs) offering the services.

The user first registers with the RC when requesting the services of the ENs corresponding to a particular AP. Then, the RC generates the appropriate key material for the AP. After this initialization, the user can now be authenticated by the AP, which will further process the request to the associated ENs. The AP is able to capture the biometric information of the user. Note that in case of a large number of users, the AP will serve as a gateway and an additional server will take over its role for user authentication and the construction of the secured response including the user's request to the ENs. For the sake of simplicity, we do not consider our explanation in this situation and limit ourselves to these four entities.

We assume that the communication between RC and user, RC and AP is secured using well established mechanisms. The RC is considered a robust and secure entity, whereas the AP and ENs in the field might be more vulnerable to tampering. The explanation will focus on the interaction between user and AP on the one hand and AP and ENs on the other hand.

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. In addition, even if one of the devices, APs or ENs 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 I: Notation for Proposed Scheme

Notation	Description
RC	Registration Center
AP	Access Point
EN_j	End Node j
U_i	User i
x, y	Secret values by RC
b	Random number
ID_i	Identity of user i
P^i_{ref}	Reference biometrics of user i
$E_k(.)/D_k(.)$	Symmetric encryption/decryption with key k
$\|$	Concatenation operator
$\oplus$	XOR operator
R_j, s_j	Output and state of PRNG in step j

C. Notations

We represent a hash function by H. The encryption operation of message m under a key K to obtain the ciphertext c is denoted as $c = E_K(m)$, and the corresponding decryption operation as $m = D_K(c)$. Furthermore, the concatenation of values m_1 and m_2 is denoted by $m_1 \| m_2$ and the xor operation by $m_1 \oplus m_2$.

We denote by S the finite set of states of the PRNG. The initial state $s_0 \in S$ is obtained after mapping with seed z. The next state function is denoted by δ and the output function by ρ producing the value R_j after step j.

VI. The system

Figure 1 presents the different phases that can be distinguished: the registration (2), the installation of APs (3) and ENs (1), the capturing of biometric data of the user (4), the actual request phase (5) and the corresponding response phase (6). We now discuss each of them into more detail. For ease in

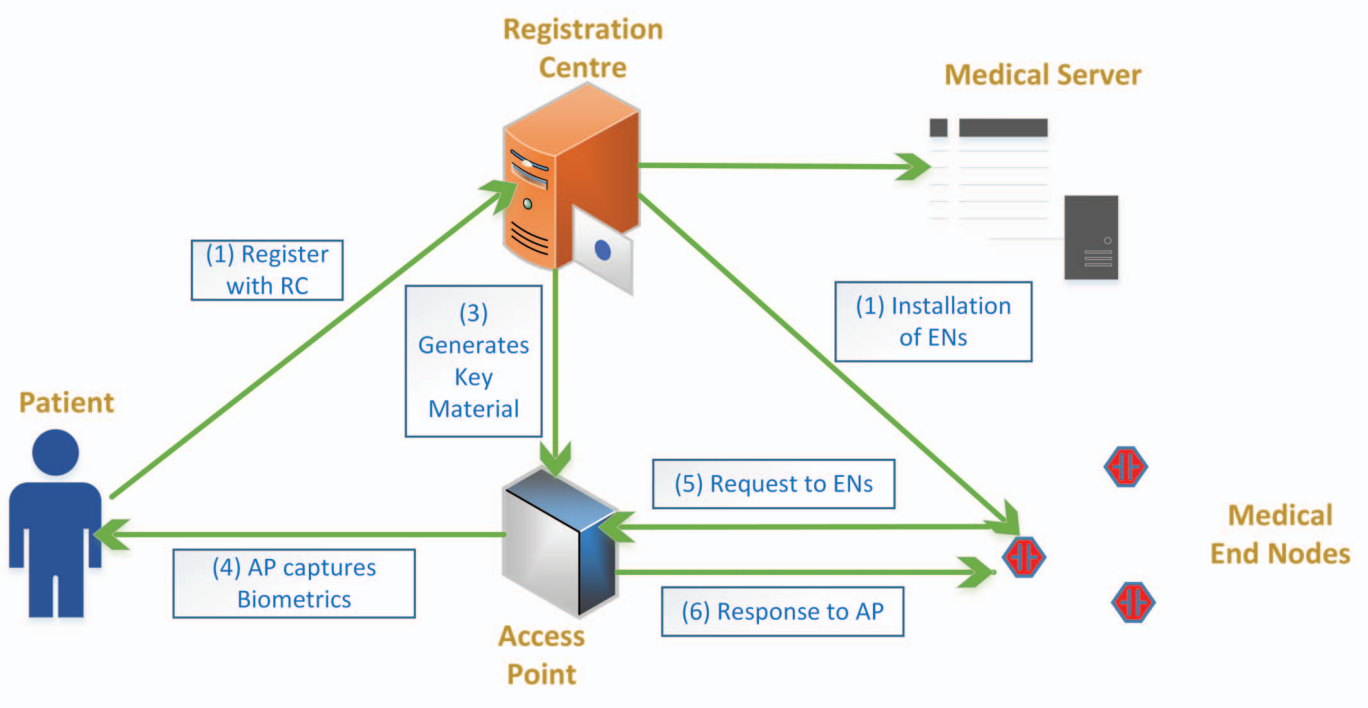

Fig. 1: Problem scenario of authentication in the Naked Environment

notations, we restrict the explication to only one AP and one end node with identity EN_j.

A. Registration phase

The RC computes a biometric characteristic of the user and generates the corresponding reference template P^i_{ref}. As it will be explained later, we choose to use an iris-based template, typically represented by 2048 bits. As studied in [18], on average half of all the bits differ for two templates of two different people, while a difference score of 0.32 statistically guarantees a positive match. We assume physical contact between user and RC in this phase in order to check the identification and authorization.

B. Installation phase

Let x, y be two secrets chosen by the RC. The RC shares the parameters $EN_j, H(x\|y), H(EN_j\|H(x))$ with each node EN_j in the network.

Before sharing secret material with the AP, RC first requests the current stage j of the PRNG at the AP. After this request, the AP updates the PRNG to the next state $j+1$. We assume that both AP and RC have the same implementation of a PRNG with the same initial seed z. Consequently, the RC can compute $R_j = \rho^{j-k}(s_k)$, where k refers to the previous stage of the PRNG. Next, the following computations are made by the RC for the registration of user U_i. Let N be the number of registrations for a user with that identity.

$$\begin{aligned} A_i &= H(y\|ID_i\|N) \\ B_i &= H(x\|y) \oplus A_i \\ C_i &= H(H(P^i_{ref})\|H(x)) \oplus H(A_i) \\ D_i &= H(x) \oplus H(P^i_{ref}) \\ E_i &= P^i_{ref} \oplus R_j \end{aligned}$$

The RC then sends the values $B_i, C_i, D_i, E_i, H(B_i\|C_i\|D_i\|E_i)$ to the AP, where they are stored. The RC also sends a list of the identities of end nodes EN_j, which are in its surrounding and can offer services for the involved user. Note that only B_i, T_e, with T_e a corresponding due date, are stored at the RC. All other intermediate computations and variables are securely erased from memory, except the latest state s_j of the PRNG.

C. Request phase

We assume the PRNG, programmed on the side of the AP, is at state s_{j+1}, and has securely stored this state s_{j+1} together with the last output value R_j in its memory. When a patient enters a room, the AP captures the biometric characteristic P^*_{ref} of the user and computes $P^*_{ref} \oplus R_j = E^*_i$. It further computes $d(E^*_i, E_i)$ for all values E_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 [18]. If successful, the process can continue and an activation of EN_j can be initiated by sending a request message to it. The biometric recognition system proposed in [19] [20] highlights the importance of distance while acquisition and matching for biometric traits.

Denote a random nonce by N_i.Following computations are made:

$$\begin{aligned} P^i_{ref} &= E_i \oplus R_j \\ H(x) &= D_i \oplus H(P^i_{ref}) \\ H(A_i) &= C_i \oplus H(H(P^i_{ref})\|H(x)) \\ C_1 &= H(EN_j\|H(x)) \oplus H(H(P^i_{ref})\|N_i) \\ C_2 &= H(A_i) \oplus N_i \\ CID_i &= B_i \oplus H(H(EN_j\|H(x))\|H(H(P^i_{ref})\|N_i)) \\ K_1 &= H(N_i \oplus B_i) \\ V_1 &= K_1 \oplus H(A_i))i \end{aligned}$$

The following message is sent to EN_j.

$$CID_i\|C_1\|C_2\|V_1 \tag{1}$$

After this process, the PRNG and the database of users is updated. This includes the following operations for the PRNG $R_{j+1} = \rho(s_{j+1})$, $s_{j+2} = \delta(s_{j+1})$. Also the value of E_i in the database for all users requires an update by replacing it to $E_i \oplus R_j \oplus R_{j+1}$, corresponding again to $E_i = P^i_{ref} \oplus R_{j+1}$. Finally, R_{j+1} and s_{j+2} must be securely stored and the other values securely erased from memory.

D. Answer phase

Here, the EN_j executes the following operations using the values stored in the memory.

$$\begin{aligned} H(H(P^i_{ref})\|N_i) &= H(EN_j\|H(x)) \oplus C_1 \\ L_i &= H(H(EN_j\|H(x))\|H(H(P^i_{ref})\|N_i)) \\ B_i &= CID_i \oplus L_i \\ A_i &= B_i \oplus H(x\|y) \\ N_i &= H(A_i) \oplus C_2 \\ K^*_1 &= H(N_i \oplus B_i) \\ H(A_i)^* &= K^*_1 \oplus V_1 \end{aligned}$$

If $H(A_i)^*$ corresponds with the transmitted value V_1, the AP and thus the user is authenticated. In case, a response is required from the end node, the following computations are performed with N_j a random value.

$$\begin{aligned} C_3 &= N_j \oplus H(H(P^i_{ref})\|N_i) \\ V_2 &= N_i \oplus H(EN_j\|B_i\|N_j) \\ SK_{ij} &= H(N_i\|N_j) \end{aligned}$$

Finally, the message $C_3\|V_2\|E_{SK_{ij}}(M)$, with M the requested info (GET request) or a confirmation (POST, DELETE, PUT request) are sent to the AP.

The AP first derives $N_j = C_3 \oplus H(H(P^i_{ref})\|N_i)$. Next $N_i \oplus H(EN_j\|B_i\|N_j)$ is calculated and compared with the transmitted value V_2. If positive, mutual authentication is obtained and the shared symmetric key can be derived in order to decrypt the last part of the message.

E. Update phase

This phase is only executed in case the user wants to update his security material. Therefore, he needs to register again to the RC, who computes his biometric characteristics.

Next, the RC generates $A_i = H(y\|ID_i\|N)$ and corresponding parameter $B_i = A_i \oplus H(x\|y)$ up to N times, until the computed B_i corresponds with the one in memory. Then, the new value for A_i is defined by $A_i = H(y\|ID_i\|N+1)$ and the corresponding updated values of B_i and C_i in memory are overwritten with their new values. The updated values of B_i, C_i are sent to the AP. Note that the value of N should be fixed dependent of the system conditions.

VII. Security analysis

Let us discuss some security features and resistance against the most relevant attacks in literature.

A. Accountability

Note that a logging mechanism should be installed in each node. Each log contains the parameters $B_i\|N_i$. The parameter B_i gives no direct information to a certain identity. However, by keeping track of the same pseudonym, abnormal behavior leading to for instance service degradation and denial of service attacks, can be more easily detected. In case of doubt, the AP or RC will be contacted to derive the identity.

B. Replay attacks

These type of attacks are avoided due to the usage of nonces. First on the side of the ENs, since logging is performed, replay attacks will be noticed. Secondly, on the side of the AP, also replay attacks will not work since the symmetric shared key with the EN is based on the first nonce, originally sent by the AP. Finally, also the RC keeps track of the number of registrations for a particular identity. One could also use timestamps, but this requires clock synchronization, which might be difficult to guarantee for low cost nodes.

C. Insider attacks

We distinguish the impact of two different situations, being a compromisd AP and EN.

1) Compromised AP: Let us assume that the attacker has physical access to the database of the AP, which stores the secret key material of all its users, being a list of valid combinations of $B_i, C_i, D_i, E_i, H(B_i\|C_i\|D_i\|E_i)$. Even in this situation, it is still impossible to formulate a valid request as the biometric information P^i_{ref} of a user U is required to retrieve the parameter $H(x)$ and the corresponding parameter $H(A_i)$. Note that we still assume that the AP has the capabilities to securely run its operations and to store the output and the next state of PRNG.

A compromised AP is also not able to derive information given by messages sent by the other APs as it is not aware of $H(x)$ and thus $H(EN_j\|H(x))$.

2) Compromised end node: A compromised end node can not take the role of AP as it does not know P^i_{ref} of the users or the parameter $H(x)$. It also does not learn anything from messages sent to another EN^*_j as it is not aware of the value $H(EN^*_j \| H(x))$.

In addition, it cannot release the critical identity related information of its users, since the received information is only indirectly associated with the user's identity. Finally, a compromised node does not have enough information to create users that can perform valid requests to other nodes, since the other secret key y is not known.

D. HW/SW attacks

The system is based on a security protocol for tamper resistant smart cards. The same ideas are applied on the side of the AP. Even with knowledge of the parameters $B_i \| C_i \| D_i \| E_i$, an attacker has no further advantage since the input of the biometric characteristic of the user is required, corresponding to the 2-factor authentication feature.

E. Identity privacy

Note that the user's request of the AP contains the parameter CID_i, which is a dynamic reference constructed by means of the nonce N_i, related to the pseudonym identity B_i of the user. Consequently, any outsider can never link the different requests to a particular user or to the same user. This also guarantees the location privacy of the user for any outside attacker.

From the request, the end node can derive the indirect link B_i with the user's identity. Only the RC is able to retrieve the real identity. Note that in contrast to an outsider, the end node has the possibility to link the requests to the same user. This feature is needed in order to easier detect abnormal behavior.

VIII. Performance Analysis

Here, we analyze the efficiency of the system, being the cost and accuracy it needs to authenticate a person in order to get access to the required services. The analysis is split in measuring the accuracy for recognition of various biometrics traits, the computational cost for cryptographic operations on the authentication protocol and the communication of the messages during the request and response phase.

A. Accuracy of biometrics computation

The accuracy of biometric characteristics can be evaluated by factors such as Equal Error Rate (EER), False Accept Rate (FAR) and False Reject Rate (FRR). The rate at which both accept and reject errors are equal, is considered as EER. FAR refers to the chances that the system inaccurately claims a valid match between the input pattern and a non-matching pattern in the database. Where as in the case of FRR, it measures the probability that the system inaccurately claims the failure of match between the input pattern and the matching template in the database. It represents the percentage of correct inputs being ruled out [21]. Table II shows the EER, FAR and FRR of various popular and frequently used biometric traits [21]. It can be seen that the iris biometrics are considered more prominent having the smallest percentages of EER, FAR and FRR in comparison with others. The artificial duplication of the iris is virtually impossible because of the uniqueness properties. Consequently, the iris biometric is suitable for the Naked environment as it is more secure, accurate than passwords and does not require hand held gadgets for capturing the iris features.

TABLE II: Accuracy of biometrics computation [21]

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%

B. Timing for cryptographic/computational operation

In this section, we have computed the computational costs for two major phases of this authentication scheme i.e. the request phase and the answer phase. The update phase is executed only when the user wants to modify the key material and thus it is not considered here. 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 [14]. 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 [22].

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 [23], 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 our results with existing remote biometric authentication schemes. The two schemes shown in [3] and [14] take higher execution time because of the need for elliptic curve point multiplication, which is not the case in our proposed scheme and the scheme of [5] as shown in Table III. The remote authentication scheme presented in [5] has quite similar computational cost compared with our scheme because it only uses hash functions. Our proposed scheme even performs better than [5], because it uses less number of hash functions and has relatively smaller execution time.

C. Communication cost

We have also calculated the communication costs for the request and answer phases of our proposed scheme and compared it with the other three available remote biometric based

TABLE III: Comparison of Computational Cost Using Our Scheme

Scheme	Request	Answer	Total	Total Time
He [3]	$5T_H$ + $2T_S$+ $1T_M$	$12T_H$ + $4T_S$+ $7T_M$	$17T_H$ + $6T_S$+ $8T_M$	13.417 ms
Baruah [5]	$6T_H$	$7T_H$	$13T_H$	0.0299 ms
Odelu [14]	$4T_H$ + $2T_S$ + $1T_M$	$13T_H$ + $4T_S$+ $5T_M$	$17T_H$ + $6T_S$+ $6T_M$	17.847 ms
Our Scheme	$6T_H$	$5T_H$	$11T_H$	0.0253 ms

TABLE IV: Comparison of Communication Cost Using Our Scheme

Scheme	Request	Answer	Total Cost
He [3]	1920 bits	1620 bits	3520 bits
Baruah [5]	640 bits	320 bits	960 bits
Odelu [14]	864 bits	2080 bits	2944 bits
Our Scheme	608 bits	448 bits	1052 bits

schemes [3, 5, 15]. 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 request phase the message $CID_i \| C_1 \| C_2 \| V_1$ needs (160+160+160+128) = 608 bits. The message at answer phase $C_3 \| V_2 \| E_{SK_{ij}}(M)$ requires (160+160+128) = 448 bits. Hence as a result, total communication overhead using our proposed scheme is 608+448 = 1052 bits. We can see that our scheme has significantly better communication costs in comparison with [3] and [14] which takes 2994 bits and 3520 bits respectively. Though our scheme possesses a slightly higher communication cost compared with the scheme of [5].

IX. Conclusions

This paper has examined the potential use case of heathcare, where, patients can access the health related services, offered by medical sensors embedded in a hospital. We assume that patients do not have any gadgets or wearables for their authentication. Biometric features play an important role in authentication of patients. Based on this problem scenario, we have proposed an efficient authentication scheme that comprises on various phases throughout the process. As the medical sensors available in the surroundings of the hospital are resource constrained, our scheme is lightweight and solely uses symmetric key based operations. Furthermore, our proposed scheme satisfies the security requirements such as confidentiality and identity privacy. Our scheme is relatively less complex in terms of computation overhead and communication when compared with some of well known existing schemes.

Acknowledgement

This work has been performed under the framework of "The Naked Approach" and "Towards Digital Paradise" projects which are funded by TEKES, Finland. Moreover, the authors would like to acknowledge the STSM Grant presented by the COST Action IC1303 AAPELE project.

References

[1] J. Aikio, V. Pentikinen, et.al., (2016), "On the Road to Digital Paradise". [Online], Available: http://nakedapproach.demoshelsinki.fi/wp-content/uploads/sites/3/2016/08/NA-concept-book.pdf

[2] "The Naked Approach, Nordic Perspective to Gadget-free Hyperconnected Environments", [Online], Available: http://nakedapproach.fi/

[3] Debiao He, Ding Wang, Robust Biometrics-Based Authentication Scheme for Multi-server Environment", IEEE Syst. J. 9 (3) (2015) 816823.

[4] Tashi, J., J.,"Comparative Analysis of Smart Card Authentication Schemes", IOSR Journal of Computer Engineering, 16(1), 91-97 (2014).

[5] Baruah, K.CH., Banerjee, S., Dutta, M.P., and Bhunia C.T., "An Improved Biometric-Based Multi Server Authentication Scheme using Smart Card", International Journal of Security and Its Application, 9(1), 397-408 (2015).

[6] Li, C.T., and Hwang, M.S., "An Efficient Biometrics Based Remote User Authentication Scheme using Smart Cards", Journal of Network and Computer Applications, 33(1), 1-5. (2010)

[7] Chuang, M.C., Chen, M.C., "An Anonymous Multi-server Authenticated Key Agreement Scheme Based on Trust Computing using Smart Cards and Biometrics", Expert Systems with Applications, 41(4), 1411-1418 (2014).

[8] Mishra, D., Das, A.K., and Mukhopadhyay, S., "A Secure User Anonoymity-Preserving Biometric-Based Multi-Server Authenticated Key Agreement Scheme using Smart Cards", Expert Systems with Applications, 41(18), 8129-8143 (2014).

[9] Das A.K., "Analysis and Improvement on an Efficient Biometric Based Remote User Authentication Scheme using Smart Cards", IET Information Security, 5(3), 145151 (2011).

[10] An, Y., "Security Analysis and Enhancements of an Effective Biometric-Based Remote User Authentication Scheme using Smart Cards", Journal of Biomedicine and Biotechnology, vol. 2012,6 pages, 2012.

[11] Khan, M.K. and Kumari, S, "An Improved Biometrics-Based Remote Authentication Scheme with User Anonymity", BioMed Research International, vol. 2013, pp. 19, 2013.

[12] Wen, F., Susilo, W., and Yang, G., "Analysis and Improvement on a Biometric-Based User Authentication Scheme using Smart Cards", Wireless Personal Communications, 80(4), 1747-1760 (2015).

[13] Braeken A., "Efficient Anonym Smart Card Based Authentication Scheme for Multi-Server Architecture", International Journal of Smart Home, 9(9), 177-184 (2015).

[14] V. Odelu, A.K. Das, A. Goswami, "A Secure Biometrics-Based Multi-Server Authentication Protocol using Smart Cards", IEEE Trans. Inf. Forensics Secur. 10 (9) (2015) 19531966.

[15] Peng Li et al., "An Alignment-free Fingerprint Cryptosystem Based on Fuzzy Vault Scheme", Journal of Network and Computer Applications, Volume 33, Issue 3, May 2010, Pages 207-220.

[16] E. Syta,et al., "Private Eyes: Secure Remote Biometric Authentication", 12th International Joint Conference on e-Business and Telecommunications (ICETE), Colmar, France 2015.

[17] pmanyu M et.al,. "Blind Authentication: A Secure Crypto-Biometric Verification Protocol", Trans Inf Forensic Secur 2010, 5(2):255-268.

[18] J. Daugman, "How Iris Recognition Works", IEEE Transactions on Circuits and Systems for Video Technology, 14(1) 2004.

[19] C. Fancourt, et al.,"Iris Recognition at a Distance", Fifth Int'l Conf. Audio Video-Based Biometric Person Authentication", pp. 1-13, NY, 2005.

[20] W. Dong, Z. Sun and T. Tan, "A Design of Iris Recognition System at a Distance", Proc. Chinese Conf. Pattern Recognition, vol. 2, pp. 553-557.

[21] D. Bhattacharyya, R. Ranjan, F. Alisherov, M. Choi, Biometric Authentication: A Review", Int. J. u- and e-Service, Sci. Technol. 2 (2009) 1328.

[22] M. Amara and A. Siad, "Elliptic Curve Cryptography and Its Applications", Proc. 7th Int. WOSSPA, pp. 247-250, Tipaza, 2011.

[23] Kilinc HH, Yanik T (2014), "A Survey of SIP Authentication and Key Agreement Schemes", IEEE Commun Surv Tutor 16(2).