BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network

Article *in* IEEE Sensors Journal · January 2015

DOI: 10.1109/JSEN.2015.2502401

Prosanta Gope

National University of Singapore

33 PUBLICATIONS **192** CITATIONS

SEE PROFILE

BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network

Prosanta Gope and Tzonelih Hwang

***Abstract*— Advances in information and communication technologies have led to the emergence of Internet of Things (IoT). In the modern health care environment, the usage of IoT technologies brings convenience of physicians and patients, since they are applied to various medical areas (such as real-time monitoring, patient information management, and healthcare management). The body sensor network (BSN) technology is one of the core technologies of IoT developments in healthcare system, where a patient can be monitored using a collection of tiny-powered and lightweight wireless sensor nodes. However, the development of this new technology in healthcare applications without considering security makes patient privacy vulnerable. In this paper, at first, we highlight the major security requirements in BSN-based modern healthcare system. Subsequently, we propose a secure IoT-based healthcare system using BSN, called BSN-Care, which can efficiently accomplish those requirements.**

***Index Terms*— BSN, data privacy, data integrity, authentication.**

I. Introduction

THE LAST few decades have witnessed a steady increase in life expectancy in many parts of the world leading to a sharp rise in the number of elderly people. A recent report from United Nations [1] predicted that there will be 2 billion (22% of the world population) older people by 2050. In addition, research indicates that about 89% of the aged people are likely to live independently. However, medical research surveys found that about 80% of the aged people older than 65 suffers from at least one chronic disease [2] causing many aged people to have difficulty in taking care of themselves. Accordingly, providing a decent quality of life for aged people has become a serious social challenge at that moment. The rapid proliferation of information and communication technologies is enabling innovative healthcare solutions and tools that show promise in addressing the aforesaid challenges.

Now, Internet of Things (IoT) has become one of the most powerful communication paradigms of the 21th century. In the IoT environment, all objects in our daily life become part of the internet due to their communication and computing capabilities (including micro controllers, transceivers for digital communication). IoT extends the concept of the Internet and makes it more pervasive. IoT allows seamless interactions among different types of devices such as medical sensor, monitoring cameras, home appliances so on. [3], [4]. Because of that reason IoT has become more productive in several areas such as healthcare system. In healthcare system, IoT involves many kinds of cheap sensors (wearable, implanted, and environment) that enable aged people to enjoy modern medical healthcare services anywhere, any time. Besides, it also greatly improves aged peoples quality of life.

The body sensor network (BSN) technology [5] is one of the most imperative technologies used in IoT-based modern healthcare system. It is basically a collection of low-power and lightweight wireless sensor nodes that are used to monitor the human body functions and surrounding environment. Since BSN nodes are used to collect sensitive (life-critical) information and may operate in hostile environments, accordingly, they require strict security mechanisms to prevent malicious interaction with the system.

In this article, at first we address the several security requirements in in BSN based modern healthcare system. Then, we propose a secure IoT based healthcare system using BSN, called BSN-Care, which can guarantee to efficiently accomplish those requirements. Therefore, the rest of the article is organized as follows. In Section II, we present a list of security parameters which are required to be addressed in any IoT based healthcare system using BSN. In Section III, we describe some of the related works in IoT based healthcare system using BSN. In Section IV, we present our BSN-Care system and subsequently, in this section, we also so show how to enforce security in our BSN-Care model to achieve all the imperative security properties. Security of the proposed scheme is analyzed in Section V. A relevant discussion based on the performance of the proposed s scheme is presented in Section VI. Finally, a concluding remark is given in Section VII. The abbreviations and cryptographic functions used in this article are defined in the Table I.

II. Security Requirements in IoT Based Healthcare System Using BSN

Security is one of the most imperative aspects of any system. People have different perspective regarding security and hence it defined in many ways. In general, security is a concept similar to safety of the system as a whole. Now, the communication in sensor network applications

Manuscript received October 29, 2015; revised November 17, 2015; accepted November 17, 2015. Date of publication November 20, 2015; date of current version February 4, 2016. This work was supported by the Ministry of Science and Technology, Taiwan, under Contract MOST 103-2221-E-006-177. The associate editor coordinating the review of this paper and approving it for publication was Prof. Subhas C. Mukhopadhyay. *(Corresponding author: Tzonelih Hwang.)*

The authors are with the Department of Computer Science and Information Engineering National Cheng Kung University, Tainan 701, Taiwan (e-mail: prosanta.nitdgp@gmail.com; hwangtl@ismail.csie.ncku.edu.tw).

Digital Object Identifier 10.1109/JSEN.2015.2502401

TABLE I

NOTATIONS AND CRYPTOGRAPHIC FUNCTIONS

Symbol	Definition
L	Local processing unit (LPU)
S	BSN-Care server
ID_L	Identity of the LPU
AID_L	One-time-alias identity of the LPU
SID	Shadow identity of the LPU
K_{ls}	Shared key between the LPU and the server
K_{em}	Shared emergency key between the LPU and the server
Tr_{Seq}	Track sequence number
LAI	Location area identifier
$h(.)$	One-way hash function
$\oplus$	Exclusive-OR operation
$\|\|$	Concatenation operation

(like BSN) in healthcare are mostly wireless in nature. This may result in various security threats to these systems. These are the security issues cloud pose serious problems to the wireless sensor devices. In this section, we describe the key security requirements in IoT based healthcare system using BSN.

A. Data Privacy

Like WSNs, data privacy is considered to be most important issue in BSN. It is required to protect the data from disclosure. BSN should not leak patient's vital information to external or neighboring networks. In IoT-based healthcare application, the sensor nodes collect and forwards sensitive data to a coordinator. An adversary can eavesdrop on the communication, and can overhear critical information. This eavesdropping may cause severe damage to the patient since the adversary can use the acquired data for many illegal purposes.

B. Data Integrity

Keeping data confidential does not protect it from external modifications. An adversary can always alter the data by adding some fragments or by manipulating the data with in a packet. This altered data can be forwarded to the coordinator. Lack of integrity mechanism is sometimes very dangerous especially in case of life-critical (when emergency data is altered). Data loss can also occur due to the bad communication environment.

C. Data Freshness

The adversary may sometimes capture data in transit and replay them later using old key in older to confuse the coordinator. Data freshness implies that data is fresh and no one can replay the old message.

D. Authentication

It is one of the most important requirements in any IoT based healthcare system using BSN, which can efficiently deal with the impersonating attacks. In BSN based healthcare system, all the sensor nodes send their data to a coordinator. Then the coordinator sends periodic updates of the patient to a server. In this context, it is highly imperative to ensure both the identity of the coordinator and the server. Authentication helps to confirm their identity to each other.

TABLE II

SECURITY RISKS TO BSN AND CORRESPONDING SECURITY REQUIREMENTS

Attack Assumptions	The Risks to BSN	Security Requirements
Computational capabilities	Data modification	Data integrity
	Impersonation	Authentication
Listening capabilities	Eavesdropping	Data privacy
	Tracking	Anonymity, Secure localization
Broadcasting capabilities	Replaying	Data freshness

E. Anonymity

A more satisfactory property of the anonymity is the untraceability, which guarantees that the adversary can neither discern who the patient is not can tell apart whether two conversations originate from same (unknown) patient. Thus, anonymity hides the source of a packet (i.e. sensor data) during wireless communication. It is a service that can enable confidentiality.

F. Secure Localization

Most BSN applications require accurate estimation of the patient location. Lack of smart tracking mechanism allows an adversary to send in correct reports about the patient location by reporting false signal strengths.

Now, in order to ensure a secure IoT-based healthcare system using BSN, it is highly imperative that the system should poses all the aforesaid security requirements and eventually can resist various security threats and attacks like data modification, impersonation, eavesdropping, replaying etc. Table II lists the various possible attacks which may occur in any IoT-based healthcare system using BSN.

III. RELATED WORK AND MOTIVATION

The advancement of BSN in healthcare applications have made patient monitoring more feasible. Recently, several wireless healthcare researches and projects have been proposed, which can aim to provide continuous patient monitoring, in-ambulatory, in-clinic, and open environment monitoring (e.g. athlete health monitoring). This section describes few popular research projects about healthcare system using body sensor networks.

CodeBlue [6], [7] is a popular healthcare research project based on BSN developed at Harvard Sensor Network Lab. In this architecture, several bio-sensors are placed on patient's body. These sensors sense the patient body and transmit it wirelessly to the end-user device (PDAs, laptops, and personal computer) for further analysis. The basic idea of the CodeBlue is straightforward, a doctor or medical professional issues a query for patient health data using their personal digital assistant (PDA), which is based on a published and subscribed architecture. Besides, CodeBlue's authors acknowledge the need of security in medical applications, but until now security is still pending or they intentionally left the security aspects for future work.

Subsequently, a heterogeneous network architecture named Alarm-net was designed at the university of Virginia [8]. The research is specifically designed for patient health monitoring in the assisted-living and home environment. Alarm-net consist of body sensor networks and environmental sensor networks. Besides, the authors have developed a circadian activity rhythms program to aid context-aware power management and privacy policies. Furthermore, Alarm-net facilitates network and data security for physiological, environment, behavioral parameters about the residents. However, Wood *et al.* [8] have pointed out some confidentiality infringement scenarios on Alarm-net, such as the fact it is susceptible to adversarial confidentiality attacks, which can leak resident's location; refer to [9] for details.

Meanwhile, Ng et al. another BSN based healthcare system UbiMon [10] was proposed in the department of computing, Imperial College, London. The aim of this project was to address the issues related to usage of wearable and implantable sensors for distributed mobile monitoring. Although Ng et al. proposed and demonstrated the ubiquitous healthcare monitoring architecture, it is widely accepted that without considering the security for wireless healthcare monitoring, which is a paramount requirement of healthcare applications, according to government laws [11].

In 2006, Chakravorty designed a mobile healthcare project called MobiCare [12]. MobiCare provides a wide-area mobile patient monitoring system that facilitates continuous and timely monitoring of the patients physiological status. Although, Chakravorty acknowledged the security issues in MobiCare, but only addressing security issues are not sufficient for real-time healthcare applications. Thus, security and privacy is still not implemented in MobiCare healthcare monitoring or may have been left out for future work. Nevertheless, there are many security issues such as secure localization, anonymity, etc, have not even mentioned in MobiCare system.

Recently, a new system designed at Johns Hopkins University named Median, especially designed for patient's monitoring in hospital and during disaster events was reported [13]. It comprises multiple physiological monitors (called PMs), which is battery powered motes and equipped with medical sensors for collecting patients' physiological health information's (e.g. blood oxygenation, pulse rate, etc.). In their description of Median its author acknowledged the need for encryption for PMs, however they did not mention which crypto-system has been used for data privacy and how they have checked the integrity of the received data. Thus, although the authors included some of the security properties to Median, their study did not reveal much information about their security implementation.

As we have seen, all the above ongoing healthcare monitoring projects enable automatic patient monitoring and provide potential quality of the healthcare without disturbing patient comfort. All the projects focus on the reliability, cost effectiveness and power consumption of their prototypes, but although most of the healthcare projects mentioned above addresses the requirement for security and privacy for sensitive data, only a few embed any security. Besides, none of the above projects addressed all the security requirements and their implication, which is greatly imperative for critical applications. Hence, it can be argued that security and privacy have not been investigated in much depth, and challenges still remain for real-time wireless healthcare application. These are the facts, greatly inspired us to propose a secure IoT based healthcare system using BSN, in which we will clearly demonstrate that how easily and efficiently to achieve all the aforesaid security requirements.

IV. Secure IoT-Based Healthcare System Using BSN (BSN-Care)

Body Sensor Network (BSN) allows the integration of intelligent, miniaturized low-power sensor nodes in, on or around human body to monitor body functions and the surrounding environment. It has great potential to revolutionize the future of healthcare technology and attained a number of researchers both from the academia and industry in the past few years. Generally, BSN consists of in-body and on-body sensor networks. An in-body sensor network allows communication between invasive/implanted devices and base station. On the other hand, an on-body sensor network allows communication between non-invasive/wearable devices and a coordinator. Now, our BSN-Care (shown in Fig. 1) is a BSN architecture composed of wearable and implantable sensors. Each sensor node is integrated with bio-sensors such as Electrocardiogram (ECG), Electromyography (EMG), Electroencephalography (EEG), Blood Pressure (BP), etc. These sensors collect the physiological parameters and forward them to a coordinator called Local Processing Unit (LPU), which can be a portable device such as PDA, smart-phone etc. The LPU works as a router between the BSN nodes and the central server called BSN-Care server, using the wireless communication mediums such as mobile networks 3G/CDMA/GPRS. Besides, when the LPU detects any abnormalities then it provides immediate alert to the person that wearing the bio-sensors. For example, in general BP less than or equal to 120 is normal, when the BP of the person reaches say 125, the LPU will provide a gentle alert to the person through the LPU devices (e.g. beep tone in a mobile phone).

When the BSN-Care server receives data of a person (who wearing several bio sensors) from LPU, then it feeds the BSN data into its database and analyzes those data. Subsequently, based on the degree of abnormalities', it may interact with the family members of the person, local physician, or even emergency unit of a nearby healthcare center. Precisely, considering a person (not necessarily a patient) wearing several bio sensors on his body and the BSN-Server receives a periodical updates from these sensors through LPU. Now, our BSN-Care server maintains an action table for each category of BSN data that it receives from LPU. Table III denotes the action table based on the data received from BP sensor, where we can see that if the BP rate is less than or equal to 120 then the server does not perform any action. Now, when the BP rate becomes greater than 130, then it informs family members of the person. If the BP rate becomes greater than 145 and there is no one attending the call in family, then the server

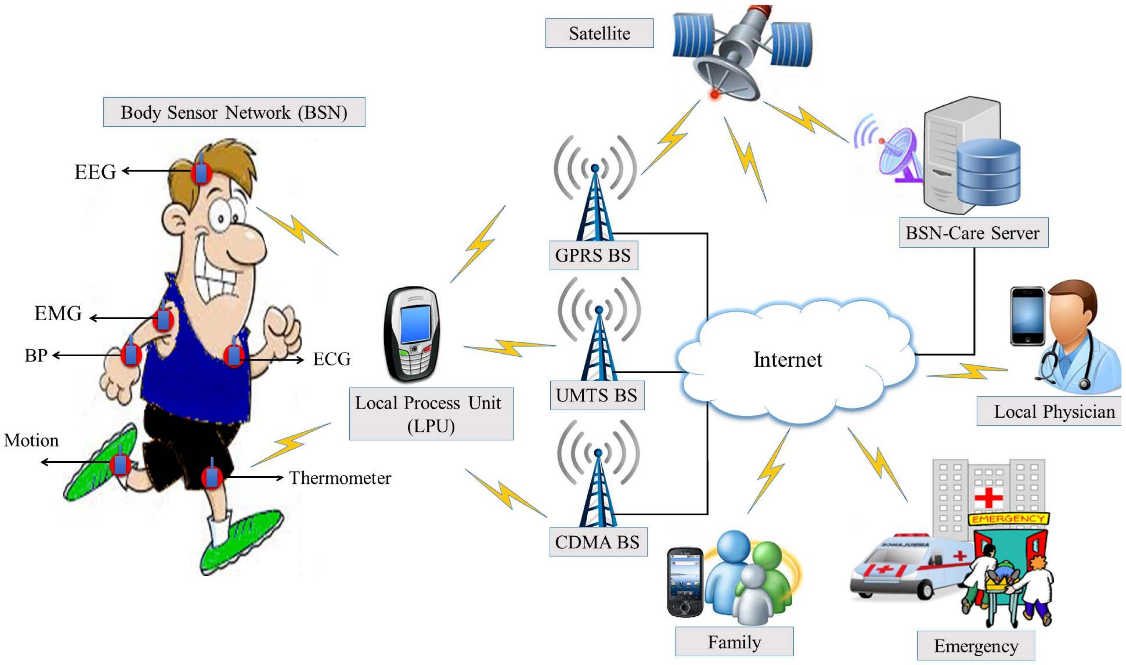


Fig. 1. Secure IoT-based modern healthcare system using BSN.

TABLE III
EXAMPLE OF ACTION TABLE USING BP DATA

BSN BP Data	Action	Response
BP≤ 120	No Action	Null
BP > 130	Inform Family Members	FR:T/F
BP > 160 and FR:F	Inform Local Physician	PR:T/F
BP >160, FR:F and PR:F	Inform Emergency	ER:T/F
FR: Family Response; **PR:**Physician Response; **ER:**Emergency Response		

will contact the local physician. Furthermore, if the BP rate of the person cross 160 and still there is no response from the family member or the local physician then the BSN-Care server will inform an emergency unit of a healthcare center and securely provides the location of the person. Here, the response parameters "FR" (Family Response), "PR" (Physician Response), and "ER" (Emergency Response) are the Boolean variables, which can be either true (T) or false (F). If the value of any response parameter is false, then the server repeats its action. For example, when the family response parameter "FR: F", then the server repeatedly call his family members. Once, the family members of the concern person pick-up the call, then the value of the family response parameter (FR) will become true i.e. "FR: T". Now, if "FR:F" and BP $>$ 130 then the BSN-Care server will call the local physician. In case, when the physician also does not respond to the server's call, then the value of the physician response parameter "PR" will stay in false. In this regard, the server will repeatedly call both the family members and the the physician. Unless any of the response parameter (FR, PR) value becomes true. Meanwhile, if "FR: F", "PR: F" and BP $>$ 160, then the BSN-Care server immediately inform to the emergency unit of a healthcare center nearest to the concern person. Once the emergency unit responds, then the value of the emergency response parameter "ER" will become true i.e. "ER: T". It should be noted that, our BSN-Care system is not only designed for the patient, instead of that it can be useful for providing a decent quality of life for the aged people.

V. ENFORCEMENT OF SECURITY IN BSN-CARE SYSTEM

We divide the all security requirements (mentioned above) into two parts: network security, and data security. Network security comprises authentication, anonymity, and secure localization. On the other hand, data security includes data privacy, data integrity, and data freshness. Now, to the best of the knowledge there is no two-party authentication protocol which can achieve all the aforesaid properties of the network security. Hence, in order to achieve all the network security requirements here we propose a lightweight anonymous authentication protocol. Subsequently, to accomplish all the data security requirements we adopt OCB authenticated encryption mode.

A. Lightweight Anonymous Authentication Protocol

In our BSN-Care system, when a LPU wants to send the periodical updates to BSN-Care server, then the server needs to confirm the identity of LPU using a lightweight anonymous authentication protocol. In this section we describe our anonymous authentication protocol in details. Our proposed authentication protocol consists of two phases: In Phase 1, the BSN-Care server issues security credentials to a LPU through secure channel, this phase is called registration phase. The next phase of the proposed authentication protocol is the anonymous authentication phase, where before data transmission from the LPU to BSN-Care server, both the LPU and the server will authenticate each other. So, the objective of our proposed lightweight authentication scheme are as follows:

- To achieve mutual authentication property.
- To achieve anonymity property.
- To achieve secure localization property.
- To defeat forgery attacks.
- To reduce computation overhead.

1) Phase I (Registration Phase): A LPU submits its identity ID_L to the BSN-Care server through a secure channel. After receiving the request from LPU, the server generates a random number N_s and then computes $K_{ls} = h(ID_L||\ N_s) \oplus ID_S$. Subsequently, the server generates a set of unlinkable shadow-IDs $SID = \{sid_1,\ sid_2, \ldots\}$, where for each $sid_j \in SID$, the server computes $sid_j = h(ID_L||r_j||K_{ls})$. Then the server also randomly generates a set of emergency keys $K_{em} = \{k_{em_1}, k_{em_2},....\}$, each corresponds to a particular $sid_j \in SID$. Hereafter, the server generates a track sequence number Tr_{Seq}, which is basically a sequence number of 32-bit. This sequence number is randomly generated. Precisely, for each request of the LPU, the server generates random number m and then sets $Tr_{Seq} = m$ and subsequently sends Tr_{Seq} to the LPU and keeps a copy in its database, in which the server can see the most recent track sequence number for each LPU ID_L registered into the system. This sequence number can be used to speed up the authentication process as well as to prevent any replay attempt from any adversary, where by seeing the Tr_{Seq} and comparing it with the stored value of its database, the server can comprehend the LPU. Here, we assume that each person wearing bio-sensor for monitoring the abnormality of any of the organ, maintain a LPU with unique identity ID_L.

Now, during the execution of the anonymous authentication phase, if the Tr_{Seq} provided by the LPU does not match with the stored value of the BSN-Care server. Then the server will immediately terminate the connection. In that case, the LPU will be asked to use it's one of the unused pair of shadow identity $sid_j \in SID$ and emergency key $k_{em_j} \in K_{em}$. Once a pair of (sid_j, k_{em_j}) is used up, then that must be deleted from the list by both the LPU and the server. Now, at the end of the registration phase, the server securely sends $\{K_{ls}, (SID, K_{em}), Tr_{Seq}, h(.)\}$ to the LPU through the secure channel and then it stores a copy of ID_L, K_{ls}, $(SID,\ K_{em})$, and Tr_{Seq} in its own database for further communication.

2) Phase II (Lightweight Anonymous Authentication Protocol): This phase achieves goals of mutual authentication among the LPU, and the server by preserving anonymity, and secure localization. This phase consists of the following steps:

Step 1: $\mathbf{M_{A_1}}$*:* LPU → Server*:* $\{AID_L,\ N_x,\ Tr_{Seq}(If\ \text{req.}),\ EL,\ V_1\}$*:*

The LPU generates a random number N_l and derives $AID_L = h(ID_L||K_{ls}||N_l||Tr_{Seq})$, $EL = LAI_l \oplus h(K_{ls}||N_l)$, $N_x = K_{ls} \oplus N_l$, $V_1 = h(N_l||LAI_l||K_{ls})$. Finally, the LPU forms a request message $\mathrm{M_{A_1}}$ and then sends it to the BSN-Care server. Here, LAI_l is the location area identifier of the base station, which represents the physical connection between the LPU and the base station of a mobile network and it will be used to provide secure localization. Note that, in case of loss of synchronization, the LPU needs to choose one of the unused pair of $(sid_j,\ k_{em_j})$ and subsequently, assigns the sid_j as AID_L i.e. $AID_L = sid_j$ and then assigns $k_{em_j} as\ K_{ls}$. In that case, LPU will not send any track sequence number Tr_{Seq} in M_{A_1}.

Step 2 $\mathbf{M_{A_2}}$*:* Server → LPU*:* $\{Tr,\ V_2,\ x(if\ \text{req.})\}$*:*

Upon receiving the request message from the LPU, the server at first checks the track sequence number Tr_{Seq} is valid or not and simultaneously also computes and checks whether the parameters V_1, AID_L, and LAI_l are valid or not. If so, then the server generates a random number m and assigns $Tr_{Seq_{new}} = m$. Subsequently, the server computes $Tr = h(K_{ls}||ID_L||N_l) \oplus Tr_{Seq_{new}}$, $V_2 = h(Tr||K_{ls}||ID_L||N_l)$ and forms a response message M_{A_2} and sends it to the LPU. Finally, the server computes $K_{ls_{new}} = h(K_{ls}||ID_L||Tr_{Seq_{new}})$ and updates its database with $Tr_{Seq} = Tr_{Seq_{new}}$, $K_{ls} = K_{ls_{new}}$. If any of the parameter is invalid then the server terminates the connection request.

Note that, in case if the server cannot find any Tr_{Seq} in M_{A_1}, then the server will validate the AID_L first, where the system will try to recognize the sid_j in AID_L. If so, then only the system (BSN-Care server) will proceed for any further computation and at the send it randomly generates a new shared key i.e. $K_{ls_{new}}$ and encodes it by using the emergency key k_{em_j} (used on that particular transaction) and the real identity of the LPU ID_L, i.e. $x = K_{ts_{new}} \oplus h(ID_L||k_{em_j})$ and sends the x with the other response parameters in $\mathrm{M_{A_2}}$.

Now, after receiving the response message $\mathrm{M_{A_2}}$ the LPU at first computes $h(Tr||K_{ls}||ID_L||N_l)$ and then verifies whether it is equals to V_2 or not. If so, then the LPU derives $Tr_{Seq_{new}} = h(K_{ls}||ID_L||N_l) \oplus Tr$, $K_{ls_{new}} = h(K_{ls}||ID_L||Tr_{Seq_{new}})$ and subsequently updates and stores $Tr_{Seq} = Tr_{Seq_{new}}$, $K_{ls} = K_{ls_{new}}$ for further communication. The pictorial description of the protocol is shown in Fig. 2.

Note that, in our BSN-Care system when a sensor needs to send some BSN data to LPU. In that case, we assume that both the sensor and the LPU can connect each other through the password-based conventional bluetooth authentication process [18]. However, our proposed lightweight two-party authentication scheme can also be used during the verification process between a sensor node and LPU.

B. Data Security in BSN-Care System

Data security is of the continuous concern in a healthcare infrastructure like BSN-Care. In fact several open questions remain. How safe and dependable are these clinical devices that are worn or implanted? How we can ensure that BSN-Care server received the unaltered data from LPU? How do we ensure data security in body sensor network?. For instance, a bio sensor sending ECG signal of a patient is error'ed or altered such that wrong diagnosis and treatment are prescribed which may cause even death. Such issues are required to be considered. Now, in order to accomplish data privacy, data integrity, and the data freshness with the reasonable computational overhead, here we adopt an authenticated encryption scheme offset codebook (OCB) mode. OCB is

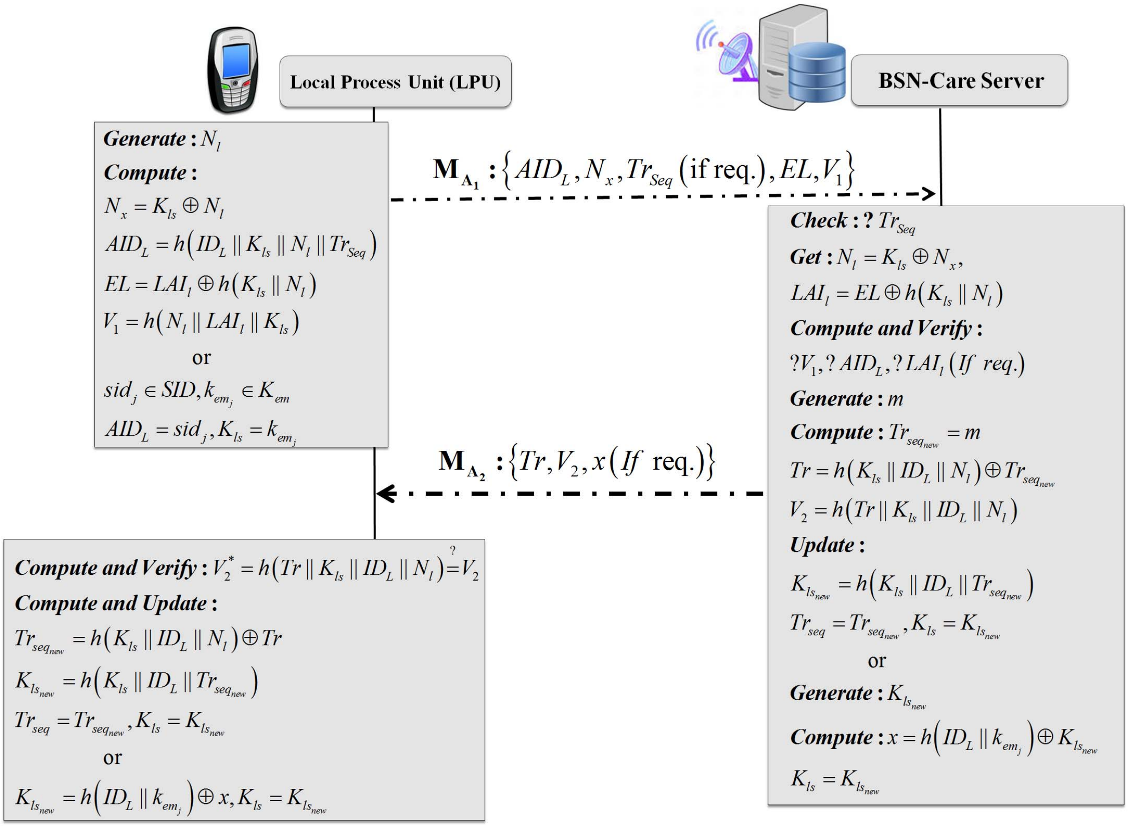

Local Process Unit (LPU)
BSN-Care Server
Generate : N_l
Compute :
$N_x = K_{ls} \oplus N_l$
$AID_L = h(ID_L \| K_{ls} \| N_l \| Tr_{Seq})$
$EL = LAI_l \oplus h(K_{ls} \| N_l)$
$V_1 = h(N_l \| LAI_l \| K_{ls})$
or
$sid_j \in SID, k_{em_j} \in K_{em}$
$AID_L = sid_j, K_{ls} = k_{em_j}$
$\mathbf{M}_{\mathbf{A}_1}: \{AID_L, N_x, Tr_{Seq}\,(\text{if req.}), EL, V_1\}$
Check : ? Tr_{Seq}
Get : $N_l = K_{ls} \oplus N_x$,
$LAI_l = EL \oplus h(K_{ls} \| N_l)$
Compute and Verify :
$?V_1, ?\,AID_L, ?\,LAI_l\,(If\ req.)$
Generate : m
Compute : $Tr_{seq_{new}} = m$
$Tr = h(K_{ls} \| ID_L \| N_l) \oplus Tr_{seq_{new}}$
$V_2 = h(Tr \| K_{ls} \| ID_L \| N_l)$
Update :
$K_{ls_{new}} = h(K_{ls} \| ID_L \| Tr_{seq_{new}})$
$Tr_{seq} = Tr_{seq_{new}}, K_{ls} = K_{ls_{new}}$
or
Generate : $K_{ls_{new}}$
Compute : $x = h(ID_L \| k_{em_j}) \oplus K_{ls_{new}}$
$K_{ls} = K_{ls_{new}}$
$\mathbf{M}_{\mathbf{A}_2}: \{Tr, V_2, x\,(If\ \text{req.})\}$
Compute and Verify : $V_2^* = h(Tr \| K_{ls} \| ID_L \| N_l) \overset{?}{=} V_2$
Compute and Update :
$Tr_{seq_{new}} = h(K_{ls} \| ID_L \| N_l) \oplus Tr$
$K_{ls_{new}} = h(K_{ls} \| ID_L \| Tr_{seq_{new}})$
$Tr_{seq} = Tr_{seq_{new}}, K_{ls} = K_{ls_{new}}$
or
$K_{ls_{new}} = h(ID_L \| k_{em_j}) \oplus x, K_{ls} = K_{ls_{new}}$

Fig. 2. Lightweight anonymous authentication protocol.

well-suited for expeditious and secure data communication, where only encryption can guarantee both the secrecy and integrity of the data in a single pass without any additional cryptographic primitive like hash function, MAC, CRC support. Hence, OCB is also well-suited for the energy constrained sensor or LPU devices. In this subsection we briefly review the OCB authenticated encryption mode.

OCB: It is a block-cipher mode of operation that features authenticated encryption, which is provably secure and is parametrized on a block cipher of block size n and a tag of τ, where τ is defined such that an adversary is able to forge a valid cipher-text with the probability of $2^{-\tau}$. OCB operates as follows. Let D be the arbitrary length data needs to be encrypted and authenticated, K be the encryption key, and N, be a non-repeating nonce. Encryption oracle of OCB takes in D, K, and N, and generates the cipher-text core C. Concurrently, using the plain-text data D; OCB generates the cipher-text C and the Tag of length τ. Now, this output pair (C, Tag) is sent to the receiving end. After receiving (C, Tag), the receiving end performs reverse operation on C to arrive at plain-text data D. Then the receiver ensures that the Tag is as expected. If the receiver computes different Tag than the once in the cipher-text, the cipher-text is considered to be invalid. In this way, if the data D is divided into n blocks, then OCB needs only $n + 1$ encryption to support both the privacy and integrity. Note that, apart from data privacy and integrity, OCB also ensures the freshness of the received data by using the incremental interface $\triangle$ where the Init (N) is the initial value for $\triangle$. This incremental interface always provides a new incremental value like a counter, which is provided through a incrementing function. Therefore, it is greatly imperative that both the sender and receiver need to use a different nonce N for each communication, it must not be repeated . For details on OCB, we refer the following paper [14].

Now, in our BSN-Care system, when sensor nodes send data to the LPU unit then they need to use OCB encryption mode with fresh nonce N and the shared key K, between the sensor nodes and the LPU. Similarly, when LPU sends the periodical updates of the sensor data then LPU also needs to use OCB mode with a fresh nonce and the updated shared key K_{ls} between the LPU and the BSN-Care server for encipher the periodic data. Therefore, when the LPU receives the data from any sensor node then apart from privacy it can also check the integrity and freshness of the data. Similarly, the BSN-Care server receives the periodic updates from LPU then it can checks the privacy, integrity, and the freshness of the received data.

VI. Security Analysis

In this section, we demonstrate that our proposed BSN-Care system can satisfy all the essential security requirements of IoT based healthcare system using BSN.

A. SR1: Accomplishment of the Mutual Authentication

Proof: In our proposed scheme, the BSN-Care server authenticates the LPU by verifying the one-time-alias identity AID_L, the track sequence number Tr_{Seq}, and the parameter V_1 in the request message of M_{A_1}, where only a legitimate LPU can form a valid request message M_{A_1}. Besides, in case of loss of synchronization, server will authenticate the LPU by using the unused shadow identity sid_j in AID_L and the value of the request parameter V_1, which must be equal to the $h(N_l||LAI_l||K_{ls})$. On the other hand, the LPU can authenticate the legitimacy of the BSN-Care server by using the parameter V_2, which must be equal to the $h(Tr||K_{ls}||ID_L||N_l)$. In this way, our proposed BSN-Care system satisfy the mutual authentication property.

B. SR2: Accomplishment of the Anonymity

Proof: In our proposed scheme, both the shadow identity with the emergency key pair and one-time-alias identity with track sequence number can resolve the issues like anonymity and untraceability. However, since the usage of (shadow-ID, emergency key) pair in each round may cause excessive storage cost in both the LPU and BSN-Care server. Therefore, the concept of (shadow-ID, emergency key) pair we only use for dealing with de-synchronization or DoS attack, which may occur because of loss of synchronization between the LPU and the server. That can be comprehended, if the response message $\mathrm{M}_{\mathrm{A}_2}$ has been interrupted, so the LPU cannot receive message within a specific time period. In that case, only a reasonable number of (shadow-identities, emergency keys) pair are required to be stored. Besides, it should be noted that, during the execution of our anonymous authentication process, none of the parameter in the request message $\mathrm{M}_{\mathrm{A}_1}$ is allowed to send twice. This approach of the proposed scheme is quite effective for privacy against eavesdropper (PAE) [16] to achieve.

C. SR3: Accomplishment of the Secure Localization

Proof: In healthcare applications, the estimation of the patient's location is very important. In real-time applications, a lack of smart tracking approach may allow an attacker to send the incorrect location by using false signals [15]. Our proposed anonymous authentication scheme can easily resolve this issue. When the BSN-Care server wants to know the patient location, then it will use the encoded location area identity i.e. EL, the server at first decodes the LAI_l from it i.e. $LAI_l = EL \oplus h(K_{ls}||N_l)$,. which represents the physical connection between the LPU and the base station of a mobile network. Subsequently, the server will also ask the base station to provide its identity i.e. LAI_l. Then the server needs to verify whether the LAI_l provided by the base station, is it equals to the LAI_l in EL or not. If the verification is successful then the sever believes the legitimacy of the base station. In other words, the signal is not false. Hereafter the server can easily locate the LPU by using the LAI_l, and eventually can reach the person having BSN.

D. SR4: Resistance to Replay and Forgery Attacks

Proof: Having intercepted previous communication, the attacker can replay the same message of the receiver or the sender to pass the verification process of the system. In our proposed authentication protocol, none of the parameter in the request message $\mathrm{M}_{\mathrm{A}_1}$ can be sent twice. Hence, if the attacker tries to intercept and resend the same request message, then by using the most recent track sequence number or a valid shadow identity, the server can easily detect it. In similar way, if the attacker attempts to send the same response message $\mathrm{M}_{\mathrm{A}_2}$ to the LPU, then the LPU can easily comprehend that. In that case, the value of the parameter V_2 will not be equal to the $h(Tr||K_{ls}||ID_L||N_l)$. In this way our proposed anonymous authentication protocol can resist replay attacks.

Now, an attacker may also attempt to intercept and modify any previous legal message of the LPU to pass the verification process of the server. In that case, the attacker needs to construct a valid request message $\mathrm{M}_{\mathrm{A}_1}$ with a valid track sequence number to pass the server's verification. However, to do that, he/she needs to extract the most recent track sequence number from Tr, i.e. $Tr = h(K_{ls}||ID_L||N_l) \oplus Tr_{Seq_{new}}$ and the attacker also needs to know the secret shared key K_{ls}, which is quite impossible for him/her to figure out these are the unknown secrets and without prior knowledge of the the attacker cannot convince the server. On the other hand, the attacker may masquerade as server to gain the benefits. In that case, the attacker needs to form a valid response message $\mathrm{M}_{\mathrm{A}_2}$ and for that also he/she needs to know the secret key K_{ls}. In this way, our proposed scheme can resist forgery attacks.

E. SR5: Accomplishment of the Data Security

Proof: As we mentioned before that data security comprises of the data privacy, data integrity, and data freshness. Due to the broadcast nature of the sensor network and wireless communication, the BSN data could easily be altered and replayed by the adversary; this cloud be dangerous in the case of life-critical events. OCB based data encryption can satisfy all the three properties of the data security, where any alternation of data and any replay attempt by an adversary can easily be detected using tag, which is unforgeable.

VII. Performance Analysis and Comparison

The purpose of the proposed scheme is to resolve several security issues existing in BSN based healthcare system and also to guarantee reasonable computational overhead. In this section, we compare our proposed BSN-Care healthcare system with the state of the art BSN based healthcare systems [8], [13] to manifest the advantages of the proposed scheme. Now, even though all the existing state-of-the-art BSN based healthcare solutions [6], [8], [10], [12], [13] addressed the requirement for security and privacy for the sensitive data, but only two of them i.e Alarm-net [8] and Median [13] embedded any security. Therefore, in order to analyze the performance of the proposed scheme especially on the security front, our proposed scheme has been compared with [8] and [13] in terms of the various security requirements of the BSN based healthcare system. From Table IV, it is clear that the proposed BSN-Care healthcare system can satisfy all the security requirements of the BSN based healthcare system.

TABLE IV
PERFORMANCE BENCHMARKING BASED ON SECURITY REQUIREMENTS

Security Requirement (SR)	Alarm-net [8]	Median [13]	BSN-Care
SR1	Yes	Yes	Yes
SR2	No	No	Yes
SR3	No	No	Yes
SR4	No	No	Yes
SR5	Yes	No	Yes

In contrast, even though both the AES-CBC encryption and CBC-MAC, used in Alarm-net and Median consider the requirement of a secure authentication scheme, but which authentication protocol they have used still unknown. Besides, none of them [6], [8], [10], [12], [13] has considered the properties like anonymity, secure localization, etc. which are greatly important. To the best of our knowledge, this is the first lightweight anonymous authentication protocol [19] for IoT based healthcare system that can guarantee all the imperative features (e.g. mutual authentication, strong user privacy preservation, secure localization) of network security.

Now, as far as the data security is concerned, Alarm-net uses the AES-CBC encryption mode and CBC-MAC in order to ensure data privacy and the data integrity, respectively. Whereas, it is still unknown how the Median checks the authenticity of the received data and which crypto-system has been used for data confidentiality. In our proposed BSN-Care healthcare system, we use OCB for ensuring the all the requirements of the data security. Here we show that our OCB-based data security approach causes significantly less computational overhead as compared AES-CBC encryption with CBC-MAC. In order to ensure privacy and integrity of the data D, divided into n blocks, our OCB based data security approach needs $\left\lceil \frac{|D|}{n} \right\rceil + 1$ block cipher calls, whereas for the same purpose AES-CBC encryption and CBC-MAC, used in Alarm-net requires $2 * \left\lceil \frac{|D|}{n} \right\rceil + 1$ to $2 * \left\lceil \frac{|D|}{n} \right\rceil + 4$ block cipher calls. In our proposed system, LPU plays a major role. It collects the sensor data and securely sends to the BSN-Care server. As we stated before that LPU can be a smartphone, or PDA. Now, in order to analyze the performance of the OCB-based data security approach with respect to the data security approach adopted in Alarm-net more precisely, here we simulate the AES-CBC block encryption and the AES-OCB block encryption environments using Java Cryptographic Extension (JCE) [17] on a smart phone of HTC Desire (considered as LPU in our BSN-Care System) with 0.72 GHZ Arm Cortex-A8 CPU and Li-Ion 1230 mAh battery as a testbed. The smartphone runs Android 2.2 mobile operating system that supports a subset of java core libraries, and in which we also install JCE. Now, using JCE with the support of the java core libraries we calculate the CPU cycles and execution time for each 128-bit block encryption. Section. Here, we take a 1024-bit of data size which is divided into eight 128-bit blocks, where each block cipher in AES-CBC takes 7.56×10^2 CPU cycles and execution time for each 128-bit block encryption of AES-CBC is 10.5×10^{-4} msec. Therefore, for ensuring both the privacy and integrity of the data size of 1024-bit using CBC encryption and CBC-MAC, respectively, the minimum computational cost and execution time that the system takes is 128.52×10^2CPU cycles and 178.5×10^{-4} msec respectively [20]. On the other hand, for the same purposes, the OCB based security approach requires only 55.12×10^2 CPU cycles and 76.55×10^{-4}msec, respectively, where for each block-cipher call in AES-OCB takes 6.89×10^2CPU cycles. Therefore, OCB-based data security approach used in our proposed BSN-Care system causes less than half computational overhead and execution time as compared to Alerm-net, which is greatly useful for the resource constrained sensor devices. The details of the comparison is shown in Figure 3 and Figure 4.

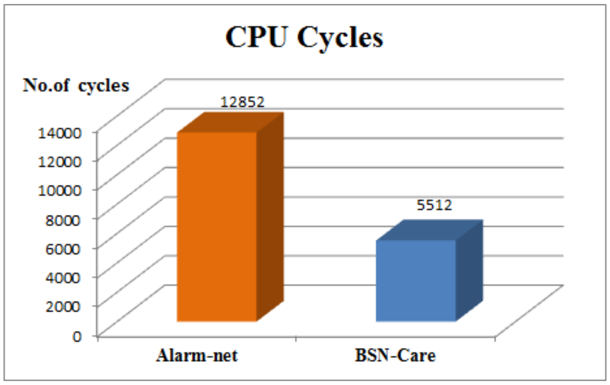


Fig. 3. Performance benchmarking based on CPU cycles.

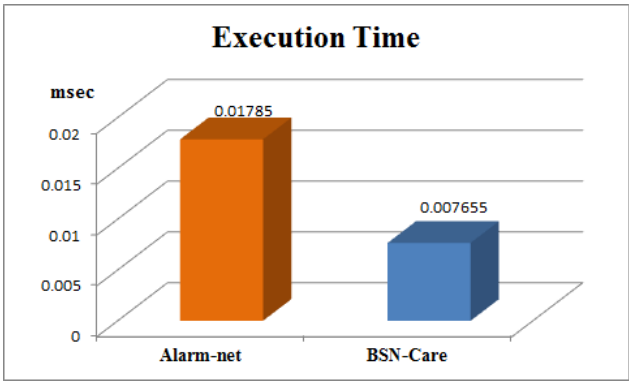


Fig. 4. Performance benchmarking based on execution time.

VIII. CONCLUSION

In this article, at first we have described the security and the privacy issues in healthcare applications using body sensor network (BSN). Subsequently, we found that even though most of the popular BSN based research projects acknowledge the issue of the security, but they fail to embed strong security services that could be preserve patient privacy. Finally, we proposed a secure IoT based healthcare system using BSN, called BSN-Care, which can efficiently accomplish various security requirements of the BSN based healthcare system.

ACKNOWLEDGMENTS

The idea of BSN-Care has been successfully implemented at ISLAB, NCKU. The authors would like to thank

Lee Chen Chang and Nieh Sheng Hung for their assistance in implementing our BSN-Care system. Finally, they also would like to sincerely thank the associate editor Subhas Mukhopadhyay and the anonymous referees for all their constructive suggestions.

References

[1] *World Population Ageing 2013*, United Nations, New York, NY, USA, 2013, pp. 8–10.

[2] R. Weinstein, "RFID: A technical overview and its application to the enterprise," *IT Prof.*, vol. 7, no. 3, pp. 27–33, May/Jun. 2005.

[3] P. Gope and T. Hwang, "Untraceable sensor movement in distributed IoT infrastructure," *IEEE Sensors J.*, vol. 15, no. 9, pp. 5340–5348, Sep. 2015.

[4] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," *Comput. Secur.*, vol. 55, pp. 271–280, Nov. 2015.

[5] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[6] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "CodeBlue: An *ad hoc* sensor network infrastructure for emergency medical care," in *Proc. MobiSys Workshop Appl. Mobile Embedded Syst. (WAMES)*, Boston, MA, USA, Jun. 2004, pp. 1–8.

[7] K. Lorincz *et al.*, "Sensor networks for emergency response: Challenges and opportunities," *IEEE Pervasive Comput.*, vol. 3, no. 4, pp. 16–23, Oct./Dec. 2004.

[8] A. Wood *et al.*, "ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring," Dept. Comput. Sci., Univ. Virginia, Charlottesville, VA, USA, Tech. Rep. CS-2006-01, 2006.

[9] S. Pai *et al.*, "Confidentiality in sensor networks: Transactional information," *IEEE Security Privacy Mag.*, vol. 6, no. 4, pp. 28–35, Jul./Aug. 2008.

[10] J. W. P. Ng *et al.*, "Ubiquitous monitoring environment for wearable and implantable sensors (UbiMon)," in *Proc. 6th Int. Conf. Ubiquitous Comput. (UbiComp)*, Nottingham, U.K., Sep. 2004, pp. 1–2.

[11] Office for Civil Rights. *United State Department of Health and Human Services Medical Privacy. National Standards of Protect the Privacy of Personal-Health-Information*. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html, accessed Jun. 15, 2011.

[12] R. Chakravorty, "A programmable service architecture for mobile medical care," in *Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshop (PERSOMW)*, Pisa, Italy, Mar. 2006, pp. 531–536.

[13] J. Ko *et al.*, "MEDiSN: Medical emergency detection in sensor networks," *ACM Trans. Embed. Comput. Syst.*, vol. 10, no. 1, pp. 1–29, Aug. 2010.

[14] P. Rogaway, M. Bellare, and J. Black, "OCB: A block-cipher mode of operation for efficient authenticated encryption," *ACM Trans. Inf. Syst. Secur.*, vol. 6, no. 3, pp. 365–403, Aug. 2003.

[15] T. Hwang and P. Gope, "Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets," *Wireless Pers. Commun.*, vol. 77, no. 1, pp. 197–224, Jul. 2014.

[16] P. Gope and T. Hwang, "Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks," *Wireless Pers. Commun.*, vol. 82, no. 4, pp. 2231–2245, Jun. 2015.

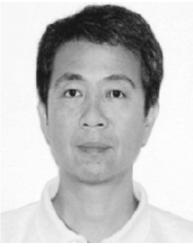
[17] Oracle Technology Network. *Java Cryptography Architecture (JCA)*. [Online]. Available: http://docs.oracle.com/javase/6/docs/technotes/guides/crypto/CrypoSpec.html, accessed Apr. 25, 2015.

[18] A. Kumar, N. Saxena, G. Tsudik, and E. Uzun, "Caveat eptor: A comparative study of secure device pairing methods," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Mar. 2009, pp. 1–10.

[19] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Syst. J.*, doi: 10.1109/JSYST.2015.2416396, 2015.

[20] T. Hwang and P. Gope, "IAR-CTR and IAR-CFB: Integrity aware real-time based counter and cipher feedback modes," in *Security and Communication Networks*. New York, NY, USA: Wiley, 2015.

Prosanta Gope received the M.Tech. degree in computer science and engineering from the National Institute of Technology, Durgapur, India, in 2009. He is currently pursuing the Ph.D. degree in computer science and information engineering with National Cheng Kung University, Tainan, Taiwan. His research interests include authentication, authenticated encryption, security in mobile communication, and cloud computing.



Tzonelih Hwang received the M.S. and Ph.D. degrees in computer science from the University of Southwestern Louisiana, USA, in 1988. He is currently a Distinguished Professor with the Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan. He has actively participated in several research activities, including a Research Scientist with the Center for Advanced Computer Studies, University of Southwestern Louisiana. He is also a Member of the Editorial Board of some reputable international journals. He has authored over 250 technical papers and holds five patents. His research interests include network and information security, access control systems, error control codes, security in mobile communication, and quantum cryptography.