Wireless Body Area Network:
From Electronic Health Security Perspective

Mohammad Javad Kargar, Department of Computer Engineering, Islamic Azad University, Maybod, Iran

Samaneh Ghasemi, Department of Computer Engineering, Islamic Azad University, Yazd, Iran

Omolbanin Rahimi, Department of Computer Engineering, Islamic Azad University, Yazd, Iran

ABSTRACT

The Wireless Body Area Network (WBAN) promises a great revolution in the field of electronic health technology in the future. These types of networks are, in fact, collections of low-priced small sensors with low voltage and computational power as well as insufficient energy capacitors which are located on the human body. As the wireless body area network should send the critical information gathered from the patient's body to the physician, the hospital, or the emergency for a supervision in real time, it needs strong mechanisms to protect the security and personal limits of the patient in order to avoid damaging invasions to the system and minimize the system vulnerability. Evaluation of previous works in WBAN security show different levels of threats and security solutions must be considered in accordance with each level. This paper aims at studying current methods of the wireless body area network and considering the levels, evaluation of the security requirements and existing threats. Furthermore, the paper is an attempt to present security solutions to improve the current status of the wireless body area network.

Keywords: *E-Health, Electronic Health Security, Security Solutions, Wireless Body Area Network (WBAN), Wireless Body Area Network (WBAN) Security*

INTRODUCTION

Thirty percent of the mortality around the globe results from cardiovascular diseases (CVD) according to statistical reports of the World Health Organization. About 17.50 million people in the world die from the heart and cerebral strokes. Also, it is predicted that about 20 million persons will die from heart diseases in 2015. More than 246 million persons throughout the world suffer from diabetes, and the figure is expected to reach 380 million people in 2025 by the population growth (Eberle, 2011) . According to the statistical reports of the USA, it is expected that the population of senior citizens older than 65 years will double by 2020, and it will triple by 2050 (Chen et al., 2011) . As a result, an increase in the age of the populations in developed countries and an increase in health care costs has urged introducing a technologi-

DOI: 10.4018/ijrqeh.2013100104

cal progress in the current methods of health care. Regardless the above mentioned, we have found out that in the current years inevitability of the electronic health for the remote health control through wireless networks and small low-power electronic systems has led to a significant development of the wireless body area networks (WBAN).

Primary applied programs of the wireless body area network initially emerged in the health and treatment area. In a way, there is a need for continuous and long term supervision on several diseases like high blood pressure, diabetes, and so on. In fact, a WBAN allows continuous supervision on physiological parameters of the patients' and lets the patient perform his/her daily activities freely and without being hospitalized for a long term. Therefore, the physician may have better control on the patient's information in such a long run. The patient's data should be sent in real time in order to help the physician to precisely diagnose the patient's problems. Furthermore, it helps the elderly to manage their daily life and medical conditions more appropriately (Wolf, 2007). As well, combination of agent features presented in Chen et al. (2011) and sensor networks in WBAN can be helpful in decision making for physicians.

The Wireless body area network entails some cheap, small, and noninvasive sensors with low voltage and computational power, and limited energy capacitors which allow a continuous supervision of the human body functions and its environment (Vallejos de Schatz et al., 2012).

Although the WBAN is typically applied in medicine, it has nonmedical applications, as well. Different applications of WBAN can be enlisted as follows:

- Supervising the health and physical fitness remotely;
- Military & Sport Trainings;
- Interactive games and entertainments;
- **Secure Identification:** This applied program includes the restoration of behavioral and mental biometric plans like the face status, finger printing, and iris diagnosis;
- Transferable audiovisual systems like microphones and MP3 players;
- Monitoring and automatic control of the physical and chemical parameters are necessary to optimize a bioprocess.

The emergence of the wireless body area network has a great potentiality in causing revolution in the future remote health technologies. Although this technology has useful effects on human quality of life, we are still encountering numerous challenges in this regard. A significant decline in power consumption is considered as one of such challenges. Indeed there has been an endeavor to minimize the battery energy in order to avoid additional costs resultant from the recharge replacement.

Saving the energy via body movement or temperature difference is one of the solutions to resolve the aforementioned issue. Besides, an increase in the sensors' dimensions rates and weight is another challenge faced in this technology. In the wireless body area network, security and efficiency of the system are very important and necessary so that designing a secure WBAN system is considered as an essential challenge for the designers (Sana Ullah, 2010). The information of a wireless body area network includes a collection of critical data gathered from different parts of the human body. In this way, the data should be transferred securely to avoid its susceptibility caused by malicious invasions to the system as such a network is being used in health and treatment areas and has a personal nature.

In a number of medical application cases, security threats might put the patient's status at risk or even cause the patient's death. Consequently, a WBAN requires strong security and scalable mechanisms to evade hostile invasions and transfer the read information reliably and precisely. As a result, the security and protection of private limits is one of the challengeable problems in WBANs.

This paper is organized in five sections. The second section elaborates on the Architecture of the wireless body area network, the third deals with the WBANs' security requirements, the fourth and fifth sections also center on different invasions and solutions for the WBANs. Finally, conclusion is presented in the final section of the paper.

THE ARCHITECTURE OF THE WIRELESS BODY AREA NETWORK

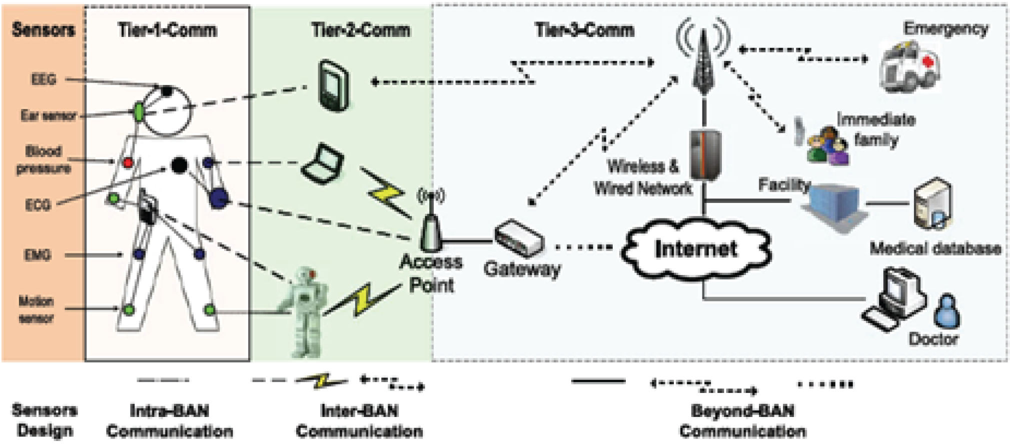
Using the available technologies like WLANs, BANs make wireless communications possible in the human body or its environment through wireless comprehensive instruments. Figure 1 exhibits the entire structure of a health-oriented care system (Chen et al., 2011). Sensors like ECG, EEG, and EMG are moveable (motional), and the blood pressure sensors, which are installed on the human body or the clothes, send their gathered data to the personal server (PS). Then the data are transferred through a WBAN communication to a medical site for the diagnosis or to a database for saving the patient's information, or to emergency alarm equipment in order to be used in critical situations. The communication structure of the BANs is divided into 3 levels: The Intra-BAN Communication, The Inter-BAN Communication, and The Beyond-BAN Communication

Each element in each level should consider different aspects like the cost, the coverage area, the bandwidth, QoS, etc. It is also required to meet such aspects considering the specific applications and the user's and market demands (Chen et al., 2011).

Intra BAN Communication

In the Intra BAN Communication, several sensors are connected together on the body, and the sensors should communicate with the PS to transfer the collected data. The design of the Intra BAN Communication is very important. Specifications like the sensors' speed and their ability to work with a battery should be considered its designing. Further, the protocol design of the Medium Access Control with low consumption and supplying Qos saving are of a high value. Yet, designing a system with all these specifications is a very demanding task. Differ-

Figure 1. Architecture of wireless body area network



ent designs have been so far presented in order to prevent the challenges of wireless connected sensors with the PS, including the SMART and MITHril project which use the cables to make connections between the existing sensors and the PS or the CodeBlue project which uses APs for connecting the sensors without a PS.

Inter BAN Communication

The communication between the PS and one or several Access Points (APs) is called the Inter BAN Communication. The PS data should be able to connect with the remote systems in order to provide such data for the physician, the emergency ward, the hospital, etc. Therefore, the Inter BAN Communication is used for the internal connection between the BANs and different networks which are accessible easily in the daily life, like cell phones, laptops, etc. These connections are divided into two classes, namely the Infrastructure and the ad-hoc. Contrary to the infrastructure which provides a reliable and wider band with a concentrated control, the ad-hoc structure shows more speed confronting an emergency case. Several wireless technologies are used for the Inter BAN Communication like the WLAN, Bluetooth, ZigBee, etc. The more technology supported by a personal server, the easier the WBAN is fused with the other applications (Otto, 2005).

THE BEYOND BAN COMMUNICATION

In the Beyond BAN Communication, the patient's medical information is sent to the database, the main element in the Beyond BAN Communication, through a cellular network or internet. This database can save the patient's medical records or profiles in order to be used by the physician in case of necessity. In addition, the physician will be able to communicate with the patient in critical situations through video conferences, and provide a proper diagnosis using the patient's saved physiological information or even warn the patient's family or the emergency ward through sending an e-mail or an SMS in emergency cases.

WBAN SECURITY REQUIREMENTS

It is necessary to comprehend the WBANs' security requirements before integrating appropriate security mechanisms. Knowing the nature of applied programs, we can use a powerful and perfect technique for protecting the system against possible security threats. WBAN-oriented programs need secure data transfer mechanisms in order to prevent the enemy from overhearing the traffic and accessing very important information of a user's. The rest of the paper proceeds with a discussion on security necessities required by the WBANs:

1. Data confidentiality

Data confidentiality is necessary to avoid disclosing and overhearing of the medical information. The premier method for implementing the data confidentiality is claimed to be the message coding. Data confidentiality guarantees that the sent packages are not being tampered by the enemy in secret (Saleem et al., 2011):

2. Data Authentication

Data validity guarantees the validity of the received message, i.e. it guarantees that the received messages are the same ones sent by the sender and just the legal nodes of the WBAN's must be able to take part in the network. Data validity allows the receiver to see whether or not the information is actually sent by the sender/a legal node (Latr et al., 2011):

3. Data Integrity

Although the received messages are being confirmed and coded, the enemy can still tamper the message on purpose. In this case, the receiver node should be able to discrete the tampered data and reject the message. Also, the data might be received in a bad physical condition, due to the damaged wireless channel. The Data integrity guarantees that the transferred data are intact and without failure (Warren et al., 2005):

4. Data freshness

Data freshness in the WBAN is very important especially when the WBAN is used for medical users. Health care programs based on WBAN play a very imperative role in the diagnosis and treatment of a patient. Loss of the medical data might prevent an effective treatment or cause death in a patient. Novelty of the data indicates that the data are received recently and guarantees that no enemies have disclosed the old messages (Liu & Kwak, 2010):

5. Data accessibility

Protecting the private and personal information against nonpermitted users is indispensable necessitating a powerful access control mechanism. The enemy may target a node by catching and depowering it so that the node results will be lost. Therefore, the operation of the sensors switch and their other operations should be protected in case of losing the node. Data accessibility guarantees the physician's easy access to the patient's information, if necessary (Li, 2010):

6. Secure Management

The coordinator needs secure management for putting the nodes distribution and coding/decoding passwords on the messages so that there will be the possibility of adding or removing the nodes in a secure environment (Vallejos de Schatz et al., 2012).

WBAN SECURITY THREATS

The WBAN should be able to improve the quality of the patient's health care without interfering with his/her comfort. In fact, medical sensors recognize the critical data of the patient's body and transfer them through wireless channels of the network. Therefore, sensitive physiological variables of the patient's should be protected against security threats and private limits. Moreover, the security of the data should be protected. For these reasons, security threats, which might damage the WBAN system are reviewed and discussed as follows.

Supervision and Overhearing the Patient' Vital Signs

Overhearing is the most widespread threat for the patient's private limits. The 'enemy' can discover the patient's information simply by searching the patient's vital signs through communication channels. Henceforth, if the enemy is equipped with a strong receiver, he can steal the messages from the network. Taking the messages may include the patient's physical situation which allows the invader to find the patient's location and hurt him/her. The enemy may discover the contents of the message including the message ID, timestamps, the origin and destination address, as well as other related information. As a result, supervision and overhearing may seriously jeopardize the individual limits of the patient (Kumar, 2011).

Information Threats While Transferring the Data

Extension of the wireless communication limit makes it vulnerable. In the WBAN, the sensors identify the patient's data and send them to the physician or the hospital server, although the sent data might be invaded. For example, the enemy may receive the physiological data through wireless channels, tamper them and put the patient at risk. There are different types of attacks while sending the data which are provided below:

1. **Interception:** Suppose that a WBAN is jeopardized by an intelligent 'enemy' so that he can illegally access the sensor's data such as the password or the ID;
2. **Message modification:** In this attack, the enemy may access the patient's wireless channels and extract their data and interfere with the obtained data deceiving the users including the physician, the nurse and the family members (Saleem et al., 2011).

Tracking the Threats in the WBAN

The WBAN needs multi-hop media to send the data from somatic sensors to a remote server so that the malicious user may invade the network. He may steal or tamper the packages and send the changed packages to the remote database causing a wrong alarm. For example, the invader might change the field address of the packages before sending them to the next hub. As a result, tracking might make a mistake or involve in an endless circle.

Distribution and Transformation Threats

In the WBAN, an invader might deceive a reliable node while sending the data to another place. The reliable node might be selected by the invader as a victim so that the node will not be secure anymore. At this instant, this node may illegally have unlimited access to the network. As the victim node is recognized by other nodes as a reliable node, it might cause a mistake alarm for the remote sites or the emergency team so that the rescue operation begins for a person who does not have any problems. In fact, a node transformation happens that may be used for service denial causing trouble in an applied program operation. Also, the patient's treatment depends on novelty of the messages received from the sensor networks. If the transformer node distributes the old data, it might result in improper treatment (like an overdose). Consequently, it can be asserted that the threats of transformation and distribution for the applied programs might be very dangerous in real time (Ameen, 2012).

Spatial Threats

Due to the fact that the mobility is one of the particulars of the WBAN's, locating the patient's precise location is necessary in emergency cases. Location tracking systems are based on radio frequencies. Therefore, the 'enemy' can locate the patient and invade his/her private limit directly if he receives the patient's radio signals and analyzes the location, permanently (Meingast, 2006).

DOS Threats

A denial of service attack or DOS is an event in which a user or an organization is deprived of receiving services from its resource that was expected in regular conditions. DOS threats may damage an applied program. Table 1 summarizes the vulnerabilities of the WBAN confronting physical layers, the data connection layer, the network layer, and the transfer layer from the OSI protocol (Saleem et al., 2010)

Physical Layer Attacks

Some of the main duties of the physical layers are the production and selection of the frequency, signal distinction, modulation, and coding:

1. **Jamming attack:** It deals with the interference of radio frequencies with the nodes. The resource of jamming attack is powerful enough to cause troubles to the network. The enemy may use several nodes to block the whole network. This attack cannot block big networks, but there is a high probability of blocking the WBAN as it is a small network;
2. **Tampering attack:** It deals with the physical attacks to the sensors. In fact, the sensors might be tampered physically by the 'enemy'. As the WBAN sensors are located in human body, the probability of

Table 1. DOS attacks in the WBAN

Layers	Dos Attacks	Defenses
Physical	Jamming	Detect and Sleep, route around jammed areas, priority messages, lower duty cycle
	Tampering	Temper-proof boxing, hiding
Data Link	Collision	Error correcting code, Authentication
	Unfairness	Small frames, anti-replay protection
	Exhaustion	Rate limitation
	Denial of sleep	Authentication and anti-replay, detect and sleep, broadcast attack protection
Network	Neglect and greed	Redundancy, probing
	Spoofing	Authentication and anti-replay protection
	Homing	Encryption
	Misdirection	Egress filtering, authorization monitoring
	Black holes	Authorization, monitoring, redundancy
	Hello floods	Pair-wise authentication, geographic routing
Transfer	Flooding	Client Puzzles, SYN cookies
	De-synchronization	Packet authentication

physical tampering in sensors is possible, accordingly (Zhang & Zhou, 2011).

Data Link Layer Attacks

This layer is responsible for the distinction of multiple data frame, and accessing to the channel and, is responsible for the system reliability:

1. **Collision attack:** Collision happens whenever two or several nodes intend to transfer the data simultaneously. In this case, the 'enemy' strategically creates an extra collision through sending repeated messages to the channel;
2. **Unfairness attack:** This attack results in a decrease in the efficiency of the network. In this case, the enemy invades through cutting the MAC priority templates;
3. **Exhaustion attack:** Exhaustion of the battery resources might happen when a victim node makes the channel busy all the time (Jang et al., 2011).

Network Layer Attacks

This network tracks the packages. Here tracking the packages between the sensors is not necessary and the packages are tracked just between the sensors and the coordinators:

1. **Spoofing attack:** The invader aims at tracking the information, changing them and making trouble in the network;
2. **Selective forwarding attack:** The invader selects a number of messages for sending and leaves the remaining alone;
3. **Sybil attack:** The invader presents more than one identity in the network;
4. **Helloflood attack:** This attack is used for deceiving the network (Saleem et al., 2011).

Transport Layer Attacks

This layer guarantees the quality and authenticity of data delivery, discovery and correction of errors:

1. **Flooding attack:** In this attack, the invader requests connection for several times until the required resources become exhausted or reach their maximum quota;
2. **De-synchronization:** The invader forges the messages exchanged between the sender and receiver or changes the MAC message confirmation code and stimulates making a request for transferring the lost frames (Jang et al., 2011).

WBAN SECURITY SOLUTIONS

Security solutions are the processes for discretion, prevention and recovery of the security attacks (Saleem et al., 2009). However, there are appropriate security mechanisms for the traditional networks which are not directly applicable for limited resources of the WBAN's. The subsequent part extensively represents the security solutions.

Encryption

Because of the fact that the WBAN includes critical physiological information, they need strong coding functions to develop security in their applied programs. These coding functions contribute to the protection of private limit and the patient's security against malevolent attacks. Strong coding depends on extensive resources and calculations. Therefore, selecting an appropriate coding method is considered as a challenge to provide the highest level of security for the network's nodes.

Secure Tracking

In the WBAN, we might need sending the data to the external source. For that reason, tracking and sending the message is a critical service for end-to-end communications. There are a lot of tracking protocols for applying in the sensor networks; nevertheless, none of them has been designed for very high security against the probable vulnerabilities. For instance, an invader may try to impose DOS attacks on tracking protocols or inject wrong tracking information to the network and cause disorder (incompatibility) in tracking. However, most of the current proposals have been designed for static somatic networks and mobility has not been considered in such protocols. As a result, applied programs are required to support tracking protocols for mobility (Saleem et al., 2011) (see Table 2).

Table 2. WBAN security threats and solutions (Saleem et al., 2009)

Security Threats	Security Requirements	Possible Security Solutions
Unauthenticated or unauthorized access	Key establishment and trust setup	Random key distribution Public key cryptography
Message disclosure	Confidentiality and privacy	Link/network layer encryption Access control
Message modification	Integrity and authenticity	Keyed secure hash function Digital signature
Denial-of-service (DoS)	Availability	Intrusion detection
Redundancy	Node capture and compromised node	Resilience to node compromise
Inconsistency detection and node revocation	Tamper-proofing	Routing attacks
Secure routing	Secure routing protocols	Intrusion and high-level security attacks

CONCLUSION

The technology of the Wireless Body Area Network is still emerging, and a lot of problems are remained to be solved. Notwithstanding the problems like the scalability, energy efficiency, the antenna design, QoS, symbiosis, and so on that we are confronted with in the WBAN, security and private limit are the most challenging issues in this regard. Security requirements and DOS threats in the WBAN are investigated in this paper. These threats may inflict serious damages on the network security and have destructive effects on the physical function, data connection, the network, and transfer layers. This paper presents a comprehensive review of the security threats and current solutions for the Wireless Body Area Network. For example, jamming attacks which deal with interfering of the radio frequencies with nodes, may cause trouble and reduce the network security. As a result, most efforts should concentrate on introducing and implementing new security levels in order to increase the security and precise protection of the private limit in the Wireless Body Area Network.

REFERENCES

Ameen, M., Liu, Jingwei, Kwak, & Kyungsup. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, *36*(1), 93–101. doi:10.1007/s10916-010-9449-4 PMID:20703745

Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. (2011). Body area networks: A survey. *Mobile Networks and Applications*, *16*(2), 171–193. doi:10.1007/s11036-010-0260-8

Chris Otto, A. M., Corey Sanders, Emil Jovanov. (2005). System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia*, *1*(4), 307–326.

Eberle, O. F. R. T. (2011). The Internet of things and its connection with wireless sensor networks. *Future Internet, 59*.

Jang, C. S., Lee, D. G., & Han, J. گ., & Park, J. H. (2011). Hybrid security protocol for wireless body area networks. *Wireless Communications and Mobile Computing*, *11*(2), 277–288. doi:10.1002/wcm.884

Kumar, P., Lee, Hoon-Jae. (2011). Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors (Basel, Switzerland)*, *12*(1), 55–91. doi:10.3390/s120100055 PMID:22368458

Latr, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A survey on wireless body area networks. *Wireless Networks*, *17*(1), 1–18. doi:10.1007/s11276-010-0252-4

Li, M., Wenjing, Lou, Kui, Ren. (2010). Data security and privacy in wireless body area networks. *Wireless Communications, IEEE, 17*(1), 51-58. doi: 10.1109/mwc.2010.5416350.

Liu, J., & Kwak, K. S. (2010). Hybrid security mechanisms for wireless body area networks. In *Proceedings of the Second International Conference on Ubiquitous and Future Networks (ICUFN)*.

Meingast, M., Roosta, T., & Sastry, S. (2006, Aug. 30 2006-Sept. 3). Security and privacy issues with health care information technology. In *Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS '06)*.

Saleem, S., Ullah, S., & Kwak, K. S. (2010). Towards security issues and solutions in wireless body area networks. In *Proceedings of the 6th International Conference on Networked Computing (INC)*.

Saleem, S., Ullah, S., & Kwak, K. S. (2011). A study of IEEE 802.15. 4 security framework for wireless body area networks. *Sensors (Basel, Switzerland)*, *11*(2), 1383–1395. doi:10.3390/s110201383 PMID:22319358

Saleem, S., Ullah, S., & Yoo, H. S. (2009). On the security issues in wireless body area networks. *JDCTA*, *3*(3), 178–184. doi:10.4156/jdcta.vol3.issue3.22

Sana Ullah, P. K., Ullah, N., Saleem, S., Higgins, H., & Sup Kwak, K. (2010). A review of wireless body area networks for medical applications. *International Journal of Communications*. *Network and System Sciences*, *3*(8), 797–803. doi: doi:10.4236/ijcns.2009.28093

Vallejos de Schatz, C. H., Medeiros, H. P., Schneider, F. K., & Abatti, P. J. (2012). Wireless medical sensor networks: Design requirements and enabling technologies. *Telemedicine and e-Health, 18*(5), 394-399.

Warren, S., Lebak, J., Yao, J., Creekmore, J., Milenkovic, A., & Jovanov, E. (2005). Interoperability and security in wireless body area network infrastructures. In *Proceedings of the 27th Annual International Conference of the Engineering in Medicine and Biology Society*. IEEE-EMBS.

Wolf, L., & Saadaoui, S. (2007, Jan. 2007). *Architecture concept of a wireless body area sensor network for health monitoring of elderly people*.

Zhang, Z., & Zhou, H. (2011). A MAC layer protocol supporting the application of WSNs in medicine and healthcare domains. In *Proceedings of the 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*.

Mohammad Javad Kargar is an Assistant Professor at the Department of Computer Engineering at Islamic Azad University, Maybod Branch in Iran. He received his Bachelor in Software Engineering, M.Sc. in Computer Architecture from University of Science and Research, and Ph.D. in Information Technology and Multimedia System from University Putra Malaysia (UPM). He has published several articles in the science –research journals such as the International Review in Computer and Software, Iranian Journal of Engineering Sciences, International Journal on Computer Science and Engineering, Australian Journal of Basic and Applied Sciences, International Journal on Internet and Distributed Computing Systems, International Journal of Advancements in Computing Technology *and* International Journal of Security and Privacy. *He has published more than 10 articles in the reputable IEEE and ACM conferences. Dr. Kargar has also been serving on the Editorial Review Board for the* International Journal of Advancements in Computing Technology *and* International Journal of Science and Advanced Technology.

Samaneh Ghasemi received his Bachelor degree from Islamic Azad University, Maybod branch. He is working for getting his Master degree in software engineering at Islamic Azad University, Yazd Banch. Her research interests include health information system and distributed systems.

Omolbanin Rahimi received his Bachelor degree from Islamic Azad University, Maybod branch. He is working for getting his Master degree in software engineering at Islamic Azad University, Yazd Banch. Her research interests include health information systems and cloud computing.