International Journal of Computer Science Engineering & Technology
APPROVED BY
NATIONAL SCIENCE LIBRARY (NSL)
NATIONAL INSTITUTE OF SCIENCE COMMUNICATION AND INFORMATION RESOURCES (NISCAIR)
COUNCIL OF SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)– NEW DELHI INDIA .
ISSN :2455-9091

SECURE ANONYMOUS AUTHENTICATION FOR WIRELESS MEDICAL SENSOR NETWORKS – A SURVEY

[1] T. Kavitha, [2] Prof. Mr. B. Loganathan
[1] Research Scholar, [2] Associate Professor,
[1] Computer Science, [2] Dept of Computer Applications,
[1, 2] Government Arts College,
[1, 2] Coimbatore, India.

ABSTRACT - An anonymous-based user authentication scheme is presented to improve the security features, computation, and communication overhead of the wireless medical sensor networks. The WMSN is one of the emerging technologies that brought revolution in many application domains such as, healthcare monitoring and so on. As the physical objects are connected via internet, security risk may arise. This paper analyses the existing technologies and protocols that are designed by different authors to ensure the secure communication over internet. It additionally focuses on the advancement in healthcare systems. It provides a summary of a large range of authentication protocols proposed in the literature. Using a multi-criteria classification previously introduced in our work, it compares and evaluates the proposed authentication protocols, showing their strengths and weaknesses, which constitutes a fundamental first step for researchers and developers addressing this domain.

Key terms: [wireless medical sensor networks, e-Healthcare Application, security, authentication.]

1. INTRODUCTION

In this architecture, medical sensors are initially placed on the body of the patient to sense and collect the related patient data, such as heartbeat rate, pulse rate, and body temperature. Thereal-time sensing data are collected using smart mobile systems by the medical professionals. However, the leakage of sensing data can encroach on the patient's privacy, and the interception has the potential to initiate data modification, which can, in turn, cause inappropriate diagnosis.
The potential exposure of personal health information is presented in through illustrations, and discussions are also provided. Unlike the traditional WSN applications, the sensed and collected data can be very sensitive, and thus, securing

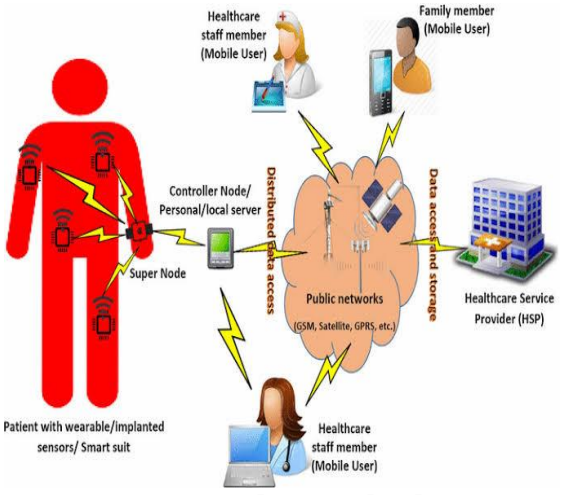

Figure 1.1 Wireless Medical Sensor Networks

The communication over WMSNs is essential. Various secure authentication

schemes have studied the security weaknesses.Such as mutual authentication, sensor node capture, offline password guessing, key impersonation, and privileged insider attacks.

Over the last decade, significant advancements have been made for Internet and mobile networks with various applications and services. Among the emerging enabling technologies, WSNs, intelligent sensing, remote sensing, low-energy wireless communications, and cloud computing (CC) have attracted the interest of computer scientists, engineers, and researchers. These technologies are also involved in other very important domains, such as health monitoring, and smart environments as well.

In, the technical opportunities offered and the technical challenges faced by the Internet of Things (IoT) are discussed considering low-energy communications and various cloud services with the main focus on IoT-enabled smart buildings.

2. SECURITY REQUIREMENTS IN HEALTHCARE SYSTEM

The health care industry gained improvements in 21stcentury due to the utilization of Wireless Body Sensor Network (WBSN) or Wireless Body Area Network (WBAN). It comprises of collection of sensor nodes that are capable of sampling, processing and communicating information. Due the evolution of m-Health, a large number of biomedical sensors which are capable of processing the physiological signs will be implanted on human body or worn by an individual in the future for the diagnosis, monitoring, and treatment of diseases.

A. Mutual authentication - It refers to a two-way authentication scheme which guarantees that only an authorized user could access services. This is one of the most fundamental requirements for IoT based health care system for enabling secure communication. It improves the overall security of the system and eliminates mimicking and spoofing attacks.

B. Data Integrity - Data Integrity ensures that the data transmitted via network is not tampered, delayed or replayed by an adversary for malicious activity. Ensuring data integrity is essential to resist against modification, repudiation and replaying attack s. Data integrity maintains the correctness and consistency of the data during the entire life cycle of the data.

C. User anonymity - To protect the user's privacy, the protocol must be able to provide user anonymity. This requirement guarantees that the attacker could never access the information of a legal party.

This keeps the identity of the patient secretive. The anonymity preservation is a very important requirement to be considered in maintaining the security of the system.

D. Availability - This requirement ensures that the server must be continuously available to the user to access information or send commands when required. Sensory data and wearable medical services must be available at all times. More significantly, data should be correct always and should be able to dynamically adapt to event, time and location and the data.

E. Non-traceability - An authentication protocol should be able to provide non-traceability; i.e., the adversary should not be able to trace the action of the valid user. The patient's location information is transmitted via communication channel.

F. Session key establishment - The session key agreement is an essential property for entity authentication and secure communication. A session key shared between two communicating parties is needed to ensure confidentiality and integrity of data. Therefore, an authentication protocol should support the session key establishment.

G. Data confidentiality - This requirement ensures that the information is transmitted securely during all communications between the communicating parties. Since the medical data are highly sensitive.As this information is highly confidential, this must be done in a secured way.

It must be encrypted both at storage and during transmission, so that users without the correct keys cannot

access the data. Therefore, the privacy of the wireless communication channels must be considered to prevent the data from eavesdropping.

H. Access control - The security mechanism must be able to properly enforce different access rights for different users. The access control mechanism must be resilient to attacks from colluding adversaries and from cloned devices.

The system should be able to verify the user and give permission to access service. For each access request, the system must verify the validity of the user. If the user is invalid, user request will not be proceed and he will not be allowed to access the services. On successful verification, the access is granted to the requester.

3. SECURE ANONYMOUS AUTHENTICATION STRATEGIES

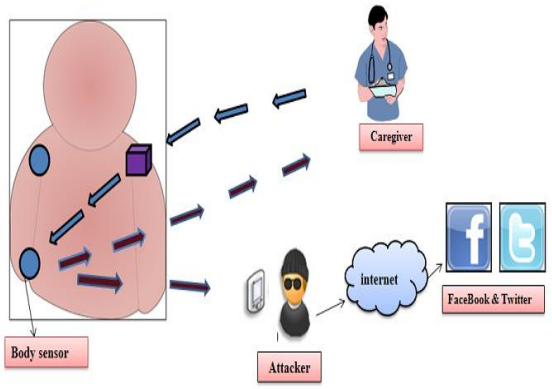

Figure 3.1 Patients Risks

Due to the growth in population, declining birth rate, rural urbanization, population aging and unbalanced resource usage, some of the social problems have become more apparent in the healthcare field which includes the inability of responding to emergency, inadequate disease prevention and early detection capability. These issues can be addressed by developing a Remote Monitoring and Management Platform which monitors, prevents and detects the diseases in human body as earlier as possible. The progress in internet technology have made patient monitoring more beneficial.

In this section, we present significant research carried out in secure anonymous authentication for wireless medical sensor networks.

BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network [3] 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 they are applied to various medical areas.

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.

A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity [6] with the development and maturation of the wireless communication technologies, the wireless sensor networks have beenwidely applied in different environments to acquire specific information. The wireless medical sensor networks (WMSNs),as a professional application of the wireless sensor networks in medicine improving the quality of healthcare services. Through the WMSNs, the parameters of patients' vital signscan be gathered from the sensor nodes equipped on the body of the patients and then can be accessed by the healthcareprofessionals by using a mobile device.

A Novel and Lightweight System to Secure Wireless Medical Sensor Networks [2] Wireless medical sensor networks (MSNs) is a key enabling technology in e-healthcare that allows the data of a patient's vital body parameters to be collected by wearable or implantable biosensors. Privacy protection of the collected data is a major unsolved issue, with challenges coming from stringent resource constraints of MSN devices, and the high demand for both security/privacy and practicality. A lightweight and secure system for MSNs. The system employs hash-chain based key updating mechanism and proxy-protected

signature technique to achieve efficient secure transmission and fine-grained data access control.

A Robust Mutual Authentication Protocol for Wireless Sensor Networks [4] Authentication is an important service in wireless sensor networks (WSNs) for an unattended environment.Recently, Das proposed a hash-based authentication protocol for WSNs, which provides more security against the masquerade, stolen-verifier, replay, and guessing attacks and avoids the threat which comes with having many logged-in users with the same login-id. In this study, we point out one security weakness of Das'protocol in mutual authentication for WSN's preservation between users, gateway-node, and sensor nodes. To remedy the problem, this paper provides a secrecy improvement over Das' protocol to ensure that a legal user can exercise a WSN in an insecure environment. Furthermore, by presenting the comparisons of security, computation and communication costs.

An Improved and Effective Secure Password-Based Authentication and Key Agreement Scheme Using Smart Cards for the Telecare Medicine Information System [10] here, we showthat though their scheme is efficient, their scheme still hastwo security weaknesses such as (1) it has design flaws inauthentication phase and (2) it has design flaws in password change phase. In order to withstand these flaws foundin Lee-Liu's scheme, we propose an improvement of theirscheme. Our improved scheme keeps also the original merits of Lee-Liu's scheme. We show that our scheme isefficient as compared to Lee-Liu's scheme. Further, throughthe security analysis, we show that our scheme is secureagainst possible known attacks.

Analysis and Enhancement of a Password Authentication and Update Scheme Based on Elliptic Curve Cryptography [17] Recently, a password authentication and update scheme has been presented by Islam and Biswas to remove the security weaknesses in Lin and Huang's scheme. Unfortunately, He et al., Wang et al., and Li have found out that Islam and Biswas' improvement was vulnerable to fine password guessing attack, stolen verifier attack, privilege insider attack, and denial of service attack. In this study, we further analyze Islam and Biswas' scheme and demonstrate that their scheme cannot resist password compromise impersonation attack. In order to remedy the weaknesses mentioned above, we propose an improved remote authentication scheme using smart card without using bilinear paring computation. Finally, we compare our enhancement is more secure and robust, while maintaining low performance cost.

Cryptanalysis and Improvement of a User Authentication Scheme Preserving Uniqueness and Anonymity for Connected Health Care [8] nowadays, connected health care applicationsare used more and more in the world. Service through theapplications can save the patients' time and expense, suchas telecare medical information system (TMIS) and integrated electronic patient record (EPR) information system.In the applications, preserving patients' privacy, transmitting messages securely and keeping mutual authenticationshould all be paid attention. Many authentication schemeshave been proposed to make a secure communicating environment.

Security Analysis and Improvement of a Privacy Authentication Scheme for Telecare Medical Information Systems [7] Authentication plays an important part to protectinformation from being attacked by malicious attackers.Recently, Jiang et al. proposed a privacy enhanced schemefor TMIS using smart cards and claimed their schemewas better than Chen et al.'s. However, we have showedthat Jiang et al.'s scheme has the weakness of ID uselessness and is vulnerable to off-line password guessingattack and user impersonation attack if an attacker compromises the legal user's smart card. Then we propose an improved mutual authentication scheme

used for a telecare medical information system. Remote monitoring, checking patients' past medical history record and medical consultant can be applied in thesystem where information transmits via Internet.

E-SAP: Efficient-Strong Authentication Protocol for Healthcare Applications Using Wireless Medical Sensor Networks [1] a wireless medical sensor network (WMSN) can sense humans' physiologicalsigns without sacrificing patient comfort and transmit patient vital signs to healthprofessionals' hand-held devices. The patient physiological data are highly sensitive andWMSNs are extremely vulnerable to many attacks. (1) atwo-factor (i.e., password and smartcard) professional authentication; (2) mutualauthentication between the professional and the medical sensor; (3) symmetricencryption/decryption for providing message confidentiality; (4) establishment of a securesession key at the end of authentication; and (5) professionals can change their password.

A Mutual Authentication Framework for Wireless Medical Sensor Networks [19] Wireless medical sensor networks (WMSN)comprise of distributed sensors, which can sense humanphysiological signs and monitor the health condition of thepatient. It is observed that providing privacy to the patient'sdata is an important issue and can be challenging. The information passing is done via the public channel in WMSN.Thus, the patient, sensitive information can be obtained byeavesdropping or by unauthorized use of handheld deviceswhich the health professionals use in monitoring the patient.Therefore, there is an essential need of restricting the unauthorized access to the patient's medical information.

CONCLUSION

This study presents various aspects of Wireless medical sensor networks (WMSN) based healthcare technologies. Since data protection and privacy of users are considered as the major challenges, researchers across the world has provided various technological solutions to enhance privacy and security mechanisms in healthcare applications.

This paper surveys on well-planned security mechanisms in WMSN based healthcare system. The basic security requirements such as health data protection, data confidentiality, data integrity, authentication etc., are addressed by the authors. In addition to these requirements, the protocols with light weight solution must also be considered to facilitate the researchers to come up with the more robust security mechanisms.

The analysis of a large spectrum of authentication protocols/schemes leads to identify a number of requirements and open issues that should be taken into consideration by researchers and developers while developing new authentication schemes for WMSN networks and applications.

REFERENCES

[1]. P. Kumar, S. Lee, and H. Lee, "E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks,"vol. 12,, Feb. 2012.

[2]. D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," vol. 18, no. 1 Jan. 2014.

[3]. P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," IEEE Sensors J., vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[4]. T. H. Chen and W. K Shih, "A robust mutual authentication protocol for wireless sensor networks," vol. 32, no. 5, 2010.

[5]. X. H. Le, M. Khalid, R. Sankar, and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare,"J. vol. 6, no. 3, pp. 355–364, 2011.

[6]. X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity,"Security 2015.

[7]. F. Wu and L. Xu, "Security analysis and improvement of a privacy authentication scheme for telecare medical information systems,"J. Med. Syst., vol. 37, no. 4, 2013.
[8]. L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," J. Med. Syst., vol. 39, no. 2, pp. 1–9, 2015.
[9]. Information technology—Smart transducer interface for sensors and actuators — Part 7: Transducer to radio frequency identification (RFID) systems communication protocols and Transducer Electronic Data Sheet (TEDS) formats, ISO/IEC/IEEE Std 21451-7, 2011.
[10]. A. K. Das and B. Bruhadeshwar, "An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system,"J. Med. Syst., vol. 37, no. 5, pp. 1–17, 2013.
[11]. H. Darrel, M. Alfred, and S. Vanstone,Guide to Elliptic Curve Cryptography. Berlin, Germany: Springer-Verlag, 2004.
[12]. N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203–209, 1987.
[13]. V. Miller, "Use of elliptic curves in cryptography," CRYPTO. Lecture Notes Comput. Sci., vol. 85, pp. 417–426, 1985.
[14]. M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," inProc. ACM Conf. Comput. Commun. Secur., 1993, pp. 62–73.
[15]. S. Mangard, E. Oswald, and F. X. Standaert, "One for alleall for one: Unifying standard differential power analysis attacks,"IET Inf. Security, vol. 5, no. 2, pp. 100–110, Jun. 2011.
[16]. T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smartcard under the threat of power analysis attacks,"IEEE Trans. Comput., vol. 51, no. 5, pp. May 2002.
[17]. L. Wang, "Analysis and enhancement of a password authentication and update scheme based on elliptic curve cryptography,"J. Appl Math., pp. 1– 11, 2014.
[18]. V. Odelu, A. K. Das, and A. Goswami, "An efficient ECC-based privacypreserving client authentication protocol with key agreement using smart card,"J. Inf. Security Appl., vol. 2, no. 1, pp. 1–1 9, 2015.
[19]. J. Srinivas, D. Mishra, and S. Mukhopadhyay, "A mutual authentication framework for wireless medical sensor networks,"JMedSyst., vol. 41, no. 5, 2017.
[20]. P. Kumar, M. Ylianttila, A. Gurtov, S. G. Lee, and H. J. Lee, "An efficient and adaptive mutual authentication framework for heterogeneous wireless sensor network-based applications,"Sensors, vol. 14, no. 2, 2014.
[21]. M. Turkanovic, B. Brumen, and M. H¨ olbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion,"Ad Hoc Netw., vol. 20, pp. 96–112, 2014.
[22]. M. S. Farash, M. Turkanovic, S. Kumaric, and M. H¨ olbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment,"AdHocNetw., vol. 36, 2016.
[23]. A. Darwish and A. E. Hassanie, "Wearable and implantable wireless sensor network solutions for healthcare monitoring,"Sensors, vol. 11, no. 6, 2011.
[24]. D. He, N. Kumar, J. Chen, C. C. Lee, N. Chilamkurti, and S. S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks,"Multimedia Syst., vol. 21, no. 1, pp. 49–60, 2013.
[25]. M. K. Khan and S. Kumari, "An improved user authentication protocol for healthcare services via wireless medical sensor networks,"Int. J. Distrib. Sens. Netw., vol. 10, no. 4, pp. 1–10, 2014.