Challenges & Security in Internet of Medical Things (IoMT) using IoT – A Review

Suniti Purbey
Computer Science & Engineering,
PhD Scholar
Amity University Chhattisgarh

Dr. B. Khandelwal
Computer Science & Engineering,
Head CSE/ IT, PhD Supervisior
Amity University Chhattisgarh

Abstract

In the current era, there's a requirement of a system with connected devices, persons, time, places and networks, which is totally incorporated in what's called as Internet of Things (IoT). Internet of Things has become the building blocks within the development of healthcare monitoring system. The aim of an efficient IoT healthcare system is to supply real time remote monitoring of patient health condition, to stop the critical patient conditions and to enhance the standard of life through smart IoT surroundings. New challenges were introduced with IoT for the safety of systems and processes and also with the privacy problems with person's medical data. Information security using IoT is extremely complicated and difficult; since global connectivity and accessibility is the the major concerns associated with IoT. Security and privacy intentionally got to be a part of any IoT use case, project or deployment. Variety of papers have worked on the access control mechanism with different techniques and with energy efficiency. Few papers have proposed different types of protocols for authentication. A system is required for the fusion of authentication protocol with energy efficient access control mechanism along with the solutions to countermeasure the attacks in security and privacy of patient healthcare data. After browsing the methodology for authentication protocol, for access control and for energy efficient access control mechanism, a combined methodology is proposed to be adopted to pool the gap.

Keywords: Internet of Things (IoT), Radio-frequency identification (RFID), Wireless body area networks (WBANs).

1. Introduction

Traditional methods of providing security can't be directly implemented in IoT's because of different standards and communication stacks involved. Information and Communication Technologies (ICTs) deployed as a part of medical information systems must assure various significant security necessities along with integrity, confidentiality, availability, non-repudiation, authentication, authorization, and accountability so on secure medical information without affecting the efficiency of services and privacy of patients' data.

Why IoT for healthcare? The main problem is that each patient, particularly living in remote locations found was unavailability of doctors and treatment on critical conditions. This had very dreadful consequences on people's mind about the hospitals and doctors services. Nowadays with the implementations of latest technologies by making use of IoT devices for healthcare monitoring system, these issues are sorted to large extent. IoT has the potential to not only keep patients safe and healthy, but to enhance how physicians deliver care too. Healthcare IoT also can boost patient engagement and satisfaction by allowing patients to spend longer interacting with their doctors. The usage of the Internet of Things (IoT) in healthcare may be a vast ecosystem. By connecting healthcare and eHealth picture, more integrated approaches and benefits are sought with a task for the so-called Internet of Healthcare Things (IoHT) or Internet of Medical Things (IoMT).

2. Literature Review:

2.1 General Definition of IoT in terms of Monitoring & Controlling in Healthcare services:

Kevin Ashton firstly proposed the concept of IoT in 1999, and he referred the IoT as uniquely identifiable interoperable connected objects with radio-frequency identification (RFID) technology (Shancang, 2015). Luigi et al. in their paper addresses the Internet of Things. Main enabling factor of this promising paradigm is that the integration of several technologies and communications solutions. Identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with subsequent Generation Internet), and distributed intelligence for smart objects are just the foremost relevant (Atzori, 2010). The fundamentals of IoT because the combination of internet and the emerging technologies has been discussed (Korteum, 2010).

She has studied that the e-Healthcare system mainly consists of three domains: body area, communication and networking, and repair. The body area domain is defined by a number of wireless body area networks (WBANs), each like a user. The major functionality of the communication and networking domain is to bridge the body area and repair domains. Advanced wireless communications technologies (e.g., cellular networks, WiFi, and WiMAX) link WBAN gateways to the web and enable efficient mutual digital communication between two WBANs. Within the service domain, a trusted authority maintains a web server that's liable for receiving, recording, and analyzing user health-related information. (Shen X., 2012).

The architecture of IoT framework and therefore the issues in design of IoT hardware and Software components (Gordana, 2017) are discussed. They elaborated the various application areas of IoT, like smart cities, healthcare, agriculture, and the nanoscale applications. (Bandyopadhyay, 2011) in their paper has studied the state-of-the art of IoT and presented the varied key technological drivers.

2.2 Capabilities of IoT for remote monitoring & controlling:

A capability has been described by (Muralidharan, 2016) in terms of varied domains:

i. Location sensing; during which RFID tags are used for tracking location.
ii. Traffic Monitoring; is employed for smart city infrastructure, where IoT provides the effective control and management of city’s traffic by using technologies, devices and the network.
iii. Environmental Monitoring; IoT helps in smart environment, by facilitating with pollution control, disaster forecast and to trigger alarm under emergency for appropriate measures.
iv. Remote e-health monitoring; through the patient’s real-time information, IoT can help in remote healthcare monitoring.

v. Remote Monitoring; is completed with IoT devices for appliances control in emergency detection, anti-theft and for energy conservation.

vi. Secure communication; IoT architecture has been developed and designed to provide suitable security and privacy features for safe and personal information's.

vii. Ad-hoc network; provides the reorganization of network to make a pervasive connectivity.

2.3 Review of Security Attacks & proposed solutions:

Jan et al. has analyzed the privacy issues within the Internet of Things intimately. To the present end, they had first discussed the evolving features and trends within the Internet of Things with the goal of scrutinizing their privacy implications. Second, had classified and examined the privacy threats within the new setting, remarking the challenges that require to be overcome to ensure that the Internet of Things becomes a reality (Ziegeldorf, 2014).

The solutions are proposed for security attacks reported for Electronics healthcare such as:

1. Masquerade attack: (Bruce, 2014) proposed an efficient, cost-effective middleware solution (that are often implemented during a wireless or wired device) to support data and network security in medical sensor networks.
2. Attacks on wearable and implantable medical devices: (Li C. R., 2011) proposed two possible defences against such attacks.
3. Body-coupled communications (BCC): (Ren, 2012) has presented an approach for exploiting social relationships that exist between individual users to detect clone attacks.
4. Accountability and revocability attack: (Yu, 2009) has proposed a way that operates to detect and reveal the identity of the key abuser.
5. Data injection attack: (Liang X. X., 2012) A distributed prediction-based secure and reliable (PSR) routing framework has been proposed for WBANs which will be integrated with a BAN routing protocol to enhance the latter's reliability and prevent data injection attacks during data communications.
6. Privacy attack: (Liang X. B., 2012) Two schemes has been proposed namely, an attribute-oriented authentication scheme and an attribute-oriented transmission scheme. (Lu, 2013) has proposed a Secure and Privacy-preserving Opportunistic Computing framework (SPOC) for m-Healthcare emergency was proposed by
7. Intra-cloud and external cloud attacks: (Garkoti, 2014) a replacement model has been proposed that mixes the functionality of digital watermarking with auditing support to enable the detection of insider attacks during a cloud based E-health environment.
8. Traffic analysis (TA) attacks: (Shen Q. L., 2014) has proposed an E-health monitoring system that ensures minimum service delay and preserves the privacy of users' health data by exploiting geo-distributed clouds.

2.4 Methods & Technologies which are used by different authors for establishment of Connection, Communication, Framework, Model, Architecture, Protocols, popular ICT paradigms etc:

It has been investigated that the likelihood of reducing the overhead of DTLS by means of 6LoWPAN header compression, and present the primary DTLS header compression specification for 6LoWPAN (Raza, 2013). A comprehensive review of up-to-date requirements in hardware, communication, and computing for next-generation uHealth systems has been presented. They compared new technological and technical trends and discussed how they address expected u-Health requirements (Touati, 2013).

The state-of-the-art approaches to designing efficient and secure eHealth monitoring has been surveyed. Specifically, they firstly presented a comprehensive framework for advanced eHealth monitoring system by describing, in detail, the whole monitoring life cycle. They need also to highlight the essential service components, with particular focus on data collection at patient side. To make sure high efficiency of the proposed framework, They have presented and analyzed the key challenges that require to be solved so as to develop efficient and secure patient-centric monitoring system (Sawand, 2015).

Firstly, the paper described the safety and therefore the privacy issues in healthcare applications using body sensor network (BSN). Subsequently, they found that even though most of the favoured BSN based research projects acknowledge the difficulty of the security, but fail to embed strong security services that would preserve patient privacy. Finally, they proposed a secure IoT based healthcare system using BSN, called BSNCare, which can efficiently accomplish various security requirements of the BSN based healthcare system (Gope, 2016).

The vulnerabilities were first studied, of the foremost recent proposed protocol for TMIS in the literature and proposed attacks supported the weaknesses associated with the misuse of the timestamp technique, the calculation of the reader request and tag response messages using the one-way hash function, which aren't attentively scrutinized. Second, they proposed an efficient dual RFID-TMIS mobile authentication protocol with high efficiency and security for healthcare systems. Their proposal has been an improvement and extension of the previous protocol where it had been proposed to associate the RFID technology with TMIS within the same authentication system to require advantages of both these two promising technologies. The performance analysis has shown that the improved protocol could solve security weaknesses of the studied protocol and supply mobility, efficiency and is compatible for TMIS adoption in remote areas and low population density (Benssalah, 2016).

A new radio-frequency identification authentication protocol has been proposed based on elliptic curve cryptography (ECC) to eliminate these vulnerabilities. Additionally, they have used an elliptic curve Diffie–Hellman (ECDH) key agreement protocol to get a temporary shared key wont to encrypt the later transmitted messages. Their protocol achieved a group of security properties likes mutual authentication, anonymity, confidentiality, forward security, location privacy, resistance of man-in-the-middle attack, resistance of replay attack and resistance of impersonation attack. They implemented a proposed protocol in real RFID system using Omni key smartcard reader (Omni key 5421) and NXP Java smartcards (J3A040). Implementation results shows that our proposed protocol outperform in term of your time complexity as compared to other similar protocols and requires less number of operations (Alamr, 2016).

A secure IoT framework has been proposed to make sure an End-To-End security from an IoT application to IoT devices. The proposed IoT framework consists of the IoT application, an IoT broker and therefore the IoT devices. The IoT devices are often deployed along a board line or a boundary of the world of IoT broker. The IoT broker manages their own devices and aggregates their sensing data. The IoT application provides users with IoT services. To use the IoT services, it must access to sensing data. Especially, the case of real-time healthcare services should consider intermediate security issues because medical information of patients is one among very sensitive privacy information. However, most of IoT protocols like CoAP and MQTT haven't any concern about the End-To-End security; they only trusted the safety of DTLS. Therefore, we proposed a replacement IoT framework to satisfy the End-To-End security feature under the CoAP communication. The proposed framework encrypts sensitive data by a symmetric encryption and an attribute-based encryption for efficiencies of communication and computation costs. In addition, each IoT device features a unique identification used together of their attributes. Consequently, although the IoT broker is one among the intermediate nodes, it decrypts and shows data as long as it satisfies all attributes (Choi, 2016).

A Secure User Profiling Structure has been presented (Ko, 2015) which has the patient information including their health information. A patient and a hospital keep it at that same time, they share the updated data. While they share the info and communicate, the data are often leaked. To unravel the safety problems, a secure channel with a hash function and an One-Time Password between a client and a hospital should be established and to get an input value to an OTP, it uses a dual hash-function. This work presents a dual hash function-based approach to get the One-Time Password ensuring a secure channel with the secured key. In result, attackers are unable to decrypt the leaked information due to the secured key; additionally, the proposed method outperforms the prevailing methods in terms of computation cost.

The Internet of Things is employed (Paschou, 2013) an idea within the health domain does not come without extra data and thus a knowledge transfer cost overheads. To affect these overheads, novel metrics, and methods are introduced in an effort to maximise the capabilities and widen acceptance/usage provided by the Internet of Things. Without losing its generality, the tactic discussed is experimentally evaluated within the paradigm of the Health domain. The main target is on the necessity for a summary of obtainable data formats and transmission methods and selection of the optimal combination, which may result to reduction/minimization of costs. An analytic methodology is presented backed with theoretical metrics and evaluated experimentally.

A number of popular ICT paradigms has been discussed (Suciu, 2016), including Cloud computing, IoT and large Data. It provided an in depth state of the art review of them and therefore the convergence between them. Next, they proposed a M2M system supported a decentralized cloud architecture, general systems and Remote Telemetry Units (RTUs) for E-Health applications. The system was built for giant processing of sensors information within the way that data are often aggregated to get B virtual sensors, and some measurement results were presented.

The patient’s data privacy concerns were identified (Sajid, 2016) and their corresponding mechanisms were also found from the chosen literature. The review revealed the very fact that, the foremost applied technique to deal with the patient’s data privacy concerns in healthcare cloud are IBE, ABE and its variants. Other techniques, that don't use any encryption strategy, are supported theoretical models and frameworks, hence are not applied in world scenario.

A lightweight break-glass access control (LiBAC) system has been proposed (Yang, 2017) which supports two ways for accessing encrypted medical files: attribute-based access and break-glass access. In normal situations, a medical worker with an attribute set satisfying the access policy of a medical file can decrypt and access the information. In emergent situations, the break-glass access mechanism bypasses the access policy of the medical file to permit timely access to the info by emergency medical aid or rescue workers.
LiBAC is lightweight since only a few calculations are executed by devices within the healthcare IoT network, and therefore the storage and transmission overheads are low. LiBAC is formally proved secure within the standard model and extensive experiments are conducted to demonstrate its efficiency.

The basic feats of NDN architecture was leveraged (Saxena, 2017)for designing and verification of an NDN-based smart health IoT (NHealthIoT) system. NHealthIoT uses pure-NDN-based M2M communication for capturing and transmission of raw sensor data to the own server which may detect emergency healthcare events using Hidden Markov Model. Emergency events are notified to the cloud server employing a novel context-aware adaptive forwarding (Cdf) strategy. Post emergency notifications, and user health information is periodically pulled by the cloud server and by other interested parties using NDN-based publish/subscribe paradigm. The cloud server carries out long-term decision making using probabilistic modeling for detecting the likelihood of chronic diseases at the early stage. They extended the workflows intuitive formal approach model for verifying the correctness of NHealthIoT during the emergency. They evaluated the cdf strategy using ndnSIM. Moreover, to validate and to point out the usability of NHealthIoT, they developed a proof-of-concept prototype test bed and evaluate it extensively. They also identified some research challenges of the NDN-IoT for researchers.

The security features has been presented (Cvitic, 2016) of each layer of the IoT architecture with the main target on perception layer specific to the IoT environment. Until the development of IoT concept, networks of sensors are utilized in enclosed information and communication systems without Internet access. Within the IoT architecture, network, middleware and application layer make integral components of the classical information and communication environments, while the perception layer is present exclusively within the IoT environment.

The weakness of an authentication protocol has been reviewed and analysed (He, 2015)for WMSNs-based healthcare application. They found that their protocol isn't correct within the authentication and session key agreement phase, such that, Ui and Sn cannot authenticate one another properly and has no thanks to agree on a session key. Besides, their protocol has no wrong password detection mechanism and should deduce the DoS problem.

The biometric has been introduced (Li X. N., 2016) because the third authentication factor, and a new user anonymous authentication protocol supported WMSNs is meant so on remove the drawbacks of the protocol of (He, 2015), Compared with previous protocols, the new presented protocol enhances the safety and also keeps the computation efficiency.

(Zhang, 2016) have analyzed the proposed scheme of (Chi, 2013) and indicated that their scheme suffers from the replay attack and possesses a flaw. Yuanyuan et al. proposed a secure energy-efficient access control scheme for wireless sensor networks to surmount the weaknesses in their scheme. Moreover, they need proved that their new scheme is secure against various sorts of attacks.

Instead of developing independent security solutions for storage and communication, (Bagci, 2016) Fusion, a framework has been proposed that gives coalesced confidential storage and communication. Fusion uses existing secure communication protocols for the IoT like Internet protocol security (IPsec) and datagram transport layer security (DTLS) and re-uses the defined communication security mechanisms within the storage component. Thus, trusted mechanisms developed for communication security are extended into the space for storing. Notably, this mechanism allows us to transmit requested data directly from the filing system without decrypting read data blocks then re-encrypting these for transmission. Thus, Fusion provides benefits in terms of processing speed and energy efficiency, which are important aspects for resource constrained IoT devices.

An innovative method (Wang, 2016) has been derived called granulometric size distribution (GSD) method supported mathematical morphology for detecting malicious attack in IoTs, like intrusion detection. They successfully generated GSD clusters to directly monitor the amount of active nodes during a wireless sensor network because the GSD curves are similar when the amount of active nodes during a wireless sensor network is fixed. Link Quality Indicator data of every node are utilized because the network parameters in this method.

Diverse aspects of IoT-based healthcare technologies (Islam, 2015) have been surveyed and presented various healthcare network architectures and platforms that support access to the IoT backbone and facilitate medical data transmission and reception. Substantial R&D efforts are made in IoT-driven health care services and applications. Additionally, the paper provides detailed research activities concerning how the IoT can address paediatric and elderly care, chronic disease supervision, private health, and fitness management. For deeper insights into industry trends and enabling technologies, the paper offers a broad view on how recent and ongoing advances in sensors, devices, internet applications, and other technologies have motivated affordablehealthcaregadgetsandconnectedhealthservicestolimitlessly expand the potential of IoT-based healthcare services for further developments. to raised understand IoT healthcare security, the paper considers various security requirements and challenges and unveils different research problems during this area to propose a model which will mitigate associated security risks. The discussion on several important issues like standardization, network type, business models, the standard of service, and health data protection is predicted to facilitate the provide a basis for further research on IoT-based healthcare services. This paper presents eHealth and IoT policies and regulations for the benefits of varied stakeholders curious about assessing IoT-based healthcare technologies.

3. Conclusion & Future Work

In this review work, we identified e-Healthcare system consisting of three domains: body area, communication and networking, and repair. After that architecture of IoT framework and therefore the issues in design of IoT hardware and software components were identified. **The grey areas identified while surveying IoT in Health Care services are following:**

1. The authentication protocols provides authentication of the user, whereas other attacks like confidentiality, integrity, repudiation, etc. were not addressed.
2. The access control mechanism provides the timely access of the network i.e. to avoid congestion within the network, but the safety issues aren't addressed.
3. A way was proposed in one paper where storage of the healthcare data is focused so on reduce the time interval of accessing the information, but security aspect isn't addressed.

Based on our analysis of the research papers in the fields of Internet of Things, we have concluded for several significant areas to be worked upon for future research. A Secure Framework/ Model/ Architecture which will integrate the hardware & software components all together for monitoring & controlling the entire health system remotely. Furthermore, a secure yet lightweight encryption scheme for cloud storage where the data can be stored which provide an entire security against different attacks along with access control and authentication protocol incorporated. So, these were the two areas that provide the most opportunity for researchers seeking to make significant improvements in the field of IoT-based healthcare.

References

[1] Alamr, A. A., Kausar, F., Kim, J., and Seo, C. (2016). A secure ECC based RFID mutual authentication protocol for internet of things. The Journal of Supercomputing, 1-14.

[2] Atzori, L., Lera, A., and Morabito, G. (2010). The Internet of things: A survey. Computer Networks, 54 (15), 2787–2805.

[3] Bagci, I. E., Raza, S., Roedig, U., and Voigt, T. (2016). Fusion: coalesced confidential storage and communication framework for the IoT. Security and Communication Networks, 9 (15), 2656-2673.

[4] Bandyopadhyay, D., Sen, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. Wireless Personal Communication, 58 (1), 49-69.

[5] Benssalah, M., Djeddou, M., and Drouiche, K. (2016). Dual cooperative RFID-telecare medicine data system authentication protocol for healthcare environments. Security And Communication Networks, 9 (18), 4924–4948.

[6] Bruce, N., Sain, M., and Lee, H.J. (2014). A support middleware solution for e healthcare system security. 16th International Conference on Advanced Communication Technology.

[7] Chi, L., Hu, L., Li, H., Sun, Y., Yuan, W., and Chu, J. (2013). Improved energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography. Sensor Letters, 11 (5), 953–957.

[8] Choi, J., In, Y., Park, C., Seok, S., Seo, H., and Kim, H. (2016). Secure IoT framework and 2D architecture for End-To-End security. Journal of Super Computing, 1-15.
[9] Cvitic, I., Vujic, M., and Husnjak, S. (2016). Classification of Security Risks within the IoT Environment. Proceedings of the 26th DAAAM International Symposium On Intelligent Manufacturing And Automation, (pp. 0731-0740).
[10] Garkoti, G., Peddoju, S. K., and Balasubramanian, R. (2014). Detection of insider attacks in cloud based e-healthcare environment. International Conference on Information Technology (ICIT2014), (pp. 195-200).
[11] Gope, P., and Hwang, T. (2016). BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network. IEEE Sensors Journal, 16 (5), 1368-1376.
[12] Gordana, G., Mladen, V., Nebojsa, M., Dragan, V., Igor, R., Slavica, T., and Milutin, R. (2017). The IoT Architectural Framework, Design Issues and Application Domains. Wireless Personal Communications, 92 (1), 127-148.
[13] He, D., Kumar, N., Chen, J., Lee, C., Chilamkurti, N., and Yeo, S. S. (2015). Robust anonymous authentication protocol for health-care International Journal of Advanced in Management, Technology and Engineering Sciences applications using wireless medical sensor networks. Multimedia Systems, 21 (1), 49-60.
[14] Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., and Kyung-Sup Kwak, K. S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access, 678-708.
[15] Ko, H., and Song, M. B. (2015). A Study on the Secure User Profiling Structure and Procedure for Home Healthcare Systems. Journal of Medical System, 42 (250), 1-9.
[16] Korteum, G., Kawsar, F., Fitton, D., and Sundramoorthy, V. (2010). Smart objects as building blocks for the Internet of Things. IEEE Internet Comput, 1 (51), 44-51.
[17] Li, C., Raghunathan, A., and Jha, N. K. (2011). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. 13th IEEE International Conference on e-Health Networking Applications and Services, (pp. 150-156).
[18] Li, X., Niu, J., Kumari, S., Liao, J., Liang, W., and Khan, M. K. (2016). A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Security and Communication Networks, 9 (15), 2643–2655.
[19] Liang, X., Barua, M., Chen, L., Lu, R., Shen, X., Li, X., and Luo, H. Y. (2012). Enabling pervasive healthcare through continuous remote health monitoring. IEEE Wireless Communications, 19 (6), 10-18.
[20] Liang, X., Xu Li, Shen, Q., Lu, R., Lin, X., Shen, X. S., and Zhuang, W. (2012). Exploiting prediction to enable secure and reliable routing in wireless body area networks. Proceedings IEEE INFOCOM, (pp. 388-396).
[21] Lu, R., Lin, X., and Shen, X. (2013). Spoc: A secure and privacy preserving opportunistic computing framework for mobile healthcare emergency. IEEE Trans. Parallel Distrib. Syst., 24 (3), 614–624.
[22] Muralidharan, S., Roy, A., and Saxena, N. (2016). An Exhaustive Review on Internet of Things from Korea's Perspective. Wireless Personal Communicatio, 90 (3), 1463–1486.
[23] Paschou, M., Sakkopoulos, E., Sourla, E., and Tsakalidis, A. (2013). Health Internet of Things: metrics and methods for efficient data transfer. Simulation Modelling Practice And Theory Elsevier , 186-189.
[24] Raza, S., Shafagh, H., Hewage, K., Hummen, R., & Voigt, T. (2013). Lithe: Lightweight secure CoAP for the internet of things. *Sensors Journal, IEEE , 13* (10), 3711–3720.
[25] Ren, Y., Chen, Y., and Chuahy, M. C. (2012). Social closeness based clone attack detection for mobile healthcare system. *IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*, (pp. 191-199).

[26] Sajid, A., and Abbas, H. (2016). Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges. *Journal of Medical System , 42* (250), https://doi.org/10.1007/s10916-015-0327-y.

[27] Sawand, A., Djahel, S., Zhang, Z., and Abdesselam, F.N. (2015). Toward Energy-Efficient and Trustworthy eHealth Monitoring System. *China Communications , 2* (1), 46-65.

[28] Saxena, D., and Raychoudhary, V. (2017). Design and Verification of an NDN-Based Safety-Critical Application: A Case Study With Smart Healthcare. *IEEE Transactions on Systems, Man, and Cybernetics:*
Systems , 1-15.

[29] Shancang, L., Li, D. X., and Shanshan, Z. (2015). The internet of things: a survey. *Information System Frontier , 17* (2), 243–259.

[30] Shen, Q., Liang, X., Shen, X. S., and Lin, X. (2014). Exploiting geo distributed clouds for a e-health monitoring system with minimum service delay and privacy preservation. *IEEE J. Biomed. Health Inf , 18* (2), 430– 439.

[31] Shen, X. (2012). Emerging technologies for e-healthcare. *IEEE Network , 26* (5), https://doi.org/10.1109/MNET.2012.6308066.

[32] Suciu, G., Suciu, V., Martian, A., Craciunescu, R., Vulpe, A., Marcu, I., Halunga, S., and Fratu, O. (2016). Big Data, Internet of Things and Cloud Convergence – An Architecture for Secure E-Health Applications. *Journal of Medical System , 42* (250), https://doi.org/10.1007/s10916-015-0327-y.

[33] Touati, F., and Tabish, R. (2013). U-Healthcare System: State-of-the-Art Review and Challenges. *Journal of Medical System* , 9949.

[34] Wang, Y., Wu, Y., and Chen, H. (2016). An intrusion detection method for wireless sensor network based on mathematical morphology. *Security and Communication Networks , 9* (15), 2744-2751.

[35] Yang, Y., Liu, X.,and Deng, R. H. (2017). Lightweight Break-glass Access Control System for Healthcare Internet-of-Things. *IEEE Transactions on Industrial Informatics.* , 1-1.

[36] Yu, S., Ren, K., Lou, W., and Li, J. (2009). Defending against Key Abuse Attacks in KP-ABE Enabled Broadcast Systems. *International Conferene on Security and Privacy in Communication Networks*, (pp. 311–329).

[37] Zeadally, S., Jesus, T., and Zubair, B. (2016). Security Attacks and Solutions in Electronic Health (E-health) Systems. *Journal of Medical System , 42* (251), 263.

[38] Zhang, Y., Kumar, N., Chen, J., and Rodrigues, J. P. C. (2016). A secure energy efficient access control scheme for wireless sensor networks based on elliptic curve cryptography. *Security and Communication Networks, 9* (17), 3944-3951.

[39] Ziegeldorf, J. H., Morchon, O.G., and Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks , 7* (12), 2728–2742.