Internet of Things for Healthcare: A Review

Kiran Dewangan[1], Dr,Mina Mishra[2]

[1]*Assistant Professor Dept. of Electronics & Telecommuincation BIT Durg*
[2] *Assistant Professor Dept. of Electronics & Telecommuincation CCET Bhilai*
[1]*kiran.dewangan@bitdurg.ac.in,* [2]*minamishraetc@gmail.com*

Abstract

In the current era, there is a requirement of a system with connected devices, persons, time, places and networks, which is completely incorporated in what is called as Internet of Things (IoT). Internet of Things has become the ultimate building blocks in the development of healthcare monitoring system. The aim of an efficient IoT healthcare system is to provide real time remote monitoring of patient health condition, to prevent the critical patient conditions and to improve the quality of life through smart IoT surroundings. New challenges have been introduced with IoT for the security of systems and processes and also with the privacy issues of person's medical data. Information security using IoT is very complicated and difficult; since global connectivity and accessibility is the major concerns related to IoT. Security and privacy by design need to be part of any IoT use case, project or deployment. A number 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 other attacks in security and privacy of patient healthcare data. After going through 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), Elliptic curve Diffie–Hellman (ECDH).*

1. Introduction

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

Why IoT for healthcare? The major problem that every 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 new technologies by making use of IoT devices for healthcare monitoring system, these issues have been sorted to huge extent. IoT has the potential to not only keep patients safe and healthy, but to improve how physicians deliver care as well. Healthcare IoT can also boost patient engagement and satisfaction by allowing patients to spend more time interacting with their doctors. The usage of the Internet of Things (IoT) in healthcare is a vast ecosystem. Within the overall connected healthcare and eHealth picture, more integrated approaches and benefits are

sought with a role for the so-called Internet of Healthcare Things (IoHT) or Internet of Medical Things (IoMT).

2. A brief review of the work already done in the field

Definition of IoT:

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 the integration of several technologies and communications solutions. Identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects are just the most relevant (Atzori, 2010). The basics of IoT as the combination of internet and the emerging technologies has been discussed (Korteum, 2010).

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

The architecture of IoT framework and the issues in design of IoT hardware and software components (Gordana, 2017) have been discussed. They have elaborated the various application areas of IoT, such as 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 various key technological drivers.

Capabilities of IoT:

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

i. Location sensing; in which RFID tags are used for tracking location.
ii. Traffic Monitoring; is used 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 done 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 private personal information's.
vii. Ad-hoc network; provides the reorganization of network to form a pervasive connectivity.

Security Attacks

Jan et al. has analyzed the privacy issues in the Internet of Things in detail. To this end, they had first discussed the evolving features and trends in the Internet of Things with the goal of scrutinizing their privacy implications. Second, had classified and examined the

privacy threats in the new setting, pointing out the challenges that need to be overcome to ensure that the Internet of Things becomes a reality (Ziegeldorf, 2014).

(Zeadally, 2016) the solutions have been proposed for security attacks reported for Electronics healthcare such as:

1. Masquerade attack: (Bruce, 2014) proposed an efficient, cost-effective middleware solution (that can be implemented in 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 defenses 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 method 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 that can be integrated with a BAN routing protocol to improve 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 new model has been proposed that combines the functionality of digital watermarking with auditing support to enable the detection of insider attacks in 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.

Methods & Technologies:

It has been investigated the possibility of reducing the overhead of DTLS by means of 6LoWPAN header compression, and present the first 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 entire monitoring life cycle. They have also highlighted the essential service components, with particular focus on data collection at patient side. To ensure high efficiency of the proposed framework, we have presented and analyzed the key challenges that need to be solved in order to develop efficient and secure patient-centric monitoring system (Sawand, 2015).

Firstly the paper described the security and the privacy issues in healthcare applications using body sensor network (BSN). Subsequently, they found that even though most of the popular BSN based research projects acknowledge the issue of the security, but fail to embed strong security services that could preserve patient privacy. Finally, they 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 (Gope, 2016).

The vulnerabilities were first studied, of the most recent proposed protocol for TMIS in the literature and proposed attacks based on the weaknesses related to the misuse of the timestamp technique, the calculation of the reader request and tag response messages

using the one-way hash function, which are not 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 was proposed to associate the RFID technology with TMIS in the same authentication system to take 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 provide mobility, efficiency and is well suited 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. In addition, they have used an elliptic curve Diffie–Hellman (ECDH) key agreement protocol to generate a temporary shared key used to encrypt the later transmitted messages. Their protocol achieved a set 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 Omnikey smartcard reader (Omnikey 5421) and NXP Java smartcards (J3A040). Implementation results shows that our proposed protocol outperform in term of time complexity as compared to other similar protocols and requires less number of operations (Alamr, 2016).

A secure IoT framework has been proposed to ensure 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 the IoT devices. The IoT devices can be deployed along a board line or a boundary of the area 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 needs to access to sensing data. Especially, the case of real-time healthcare services should consider intermediate security issues because medical information of patients is one of very sensitive privacy information. However, most of IoT protocols such as CoAP and MQTT have no concern about the End-To-End security; they only depended on the security of DTLS. Therefore, we proposed a new 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 has a unique identification used as one of their attributes. Consequently, although the IoT broker is one of the intermediate nodes, it decrypts and shows data only if 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 data and communicate, the data can be leaked. To solve the security problems, a secure communication channel with a hash function and an One-Time Password between a client and a hospital should be established and to generate an input value to an OTP, it uses a dual hash-function. This work presents a dual hash function-based approach to generate the One-Time Password ensuring a secure communication channel with the secured key. In result, attackers are unable to decrypt the leaked information because of the secured key; in addition, the proposed method outperforms the existing methods in terms of computation cost.

The Internet of Things is used (Paschou, 2013) a concept in the health domain does not come without extra data and therefore a data transfer cost overheads. To deal with these overheads, novel metrics, and methods are introduced in an attempt to maximize the capabilities and widen acceptance/usage provided by the Internet of Things. Without losing its generality, the method discussed is experimentally evaluated in the paradigm of the Health domain. The focus is on the need for an overview of available data formats and transmission methods and selection of the optimal combination, which can 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 Big Data. It provided an extensive state of the art review of them and the convergence between them. Next, they proposed a M2M system based on a decentralized cloud architecture, general systems and Remote Telemetry Units (RTUs) for E-Health applications. The system was built for Big Data processing of sensors information in the way that data can be aggregated to generate 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 selected literature. The review revealed the fact that, the most applied technique to address the patient's data privacy concerns in healthcare cloud are IBE, ABE and its variants. Other techniques, that do not use any encryption strategy, are based on theoretical models and frameworks, hence are not applied in real 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 data. In emergent situations, the break-glass access mechanism bypasses the access policy of the medical file to allow timely access to the data by emergency medical care or rescue workers. LiBAC is lightweight since very few calculations are executed by devices in the healthcare IoT network, and the storage and transmission overheads are low. LiBAC is formally proved secure in 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 home server which can detect emergency healthcare events using Hidden Markov Model. Emergency events are notified to the cloud server using 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 possibility 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 show the usability of NHealthIoT, they developd a proof-of-concept prototype testbed 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 focus on perception layer specific to the IoT environment. Until the development of IoT concept, networks of sensors are used 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 analyzed (He, 2015)for WMSNs-based healthcare application. They found that their protocol is not correct in the authentication and session key agreement phase, such that, Ui and Sn cannot authenticate each other properly and has no way to agree on a session key. Besides, their protocol has no wrong password detection mechanism and may deduce the DoS problem. The biometric has been introduced (Li X. N., 2016) as the third authentication factor, and a new user anonymous authentication protocol based on WMSNs is designed so as to remove the drawbacks of the protocol of (He, 2015), Compared with previous protocols, the new presented protocol enhances the security 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 have proved that their new scheme is secure against various types of attacks.

Instead of developing independent security solutions for storage and communication, (Bagci, 2016) Fusion, a framework has been proposed that provides coalesced confidential storage and communication. Fusion uses existing secure communication protocols for the IoT such as 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 storage space. Notably, this mechanism allows us to transmit requested data directly from the file system without decrypting read data blocks and 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 based on mathematical morphology for detecting malicious attack in IoTs, such as intrusion detection. They successfully generated GSD clusters to directly monitor the number of active nodes in a wireless sensor network because the GSD curves are similar when the number of active nodes in a wireless sensor network is fixed. Link Quality Indicator data of each node are utilized as 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 have been made in IoT-driven health care services and applications. In addition, the paper provides detailed research activities concerning how the IoT can address pediatric 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 better understand IoT healthcare security, the paper considers various security requirements and challenges and unveils different research problems in this area to propose a model that can mitigate associated security risks. The discussion on several important issues such as standardization, network type, business models, the quality of service, and health data protection is expected 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 various stakeholders interested in assessing IoT-based healthcare technologies.

3. Identify the Problem:

The problems identified in the above research papers are:

1. The authentication protocols provides authentication of the user, whereas other attacks like confidentiality, integrity, repudiation, etc are not addressed.
2. The access control mechanism provides the timely access of the network i.e. to avoid congestion in the network, but the security issues are not addressed.
3. A method was proposed in one paper where storage of the healthcare data is focused so as to reduce the processing time of accessing the data, but security aspect is not addressed.

4. Conclusion

With the above problems identified a system still needs to be designed where the physician at other location can analyze the real time patient's vital parameters through secure mechanisms. A system needs to be designed so as to provide a complete security against different attacks, with access control and authentication protocol incorporated for 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 information 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*, (p. https://doi.org/10.1109/ICACT.2014.6778919).

[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 in 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

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 Communication , 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.