ISSN: 2393-8528

IJICSE
Open Access
Journal Approved by UGC

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 4 Issue 4; July-August-2017; Page No. 22-28

# Survey on security of Internet of Things in eHealth and clouds

**N.Sriram**

Assistant Professor, KG College of Arts and Science, Saravanampatti, Coimbatore – 35.

sriram.n@kgcas.com

Received 10 May 2017; Accepted 04 July. 2017

**ABSTRACT**

The technology of Internet of Things (IoT) and cloud has exposed devices to vulnerabilities. As they are distributed, the different devices communicate real time information to open, private or hybrid clouds, with the possibility of collecting, storing and analyzing big data streams in new forms. In the healthcare context, the increased deployment of IoT devices makes patient information a subject to malicious attacks depending on the security and privacy of the IoT devices. While a number of researchers have explored such security challenges and open problems in IoT, there is a lack of a systematic study of the security challenges in the IoT for eHealth on clouds. In this paper, we aim at bridging this gap by conducting a thorough analysis of IoT security Vulnerability. We present then security challenges in the cloud for eHealth domain and recent proposed solutions. We also provide a proposition of an IoT system in the cloud.

**Keywords:** IoT, Cloud, e-health, Security

## Introduction

Providing better healthcare services and improving the quality of life of people presents a primary focus of research, healthcare systems using distributed services based on emerging communication technologies and advanced software architecture, are called eHealth systems. The eHealth services provide a great wealth of formation that can be used to make better actionable decisions. By connecting information, people, devices, processes and context, next generation eHealth services making use of Iot and cloud computing technologies are being developed [1].

Using the cloud technology in the eHealth domain has improved quality of services thanks to the cloud characteristics such as economical, scalable, expedient, ubiquitous, and on-demand access to shared resources [2, 3]. Cloud computing improves efficiency healthcare not only by the use of different medical resources but also with achieving a strong information technology resources and optimizing patient flow [1].

The Internet of Things (IoT) is defined by the European Commission Information Society, as a manageable set of convergent development in sensing, identification, communication, networking, and informatics devices and systems [41]. IoT devices include personal computers, sensors, tablets, smart phones, and other embedded systems. At a conceptual level, IoT refers to the inter connectivity among different devices, which enables the capturing of real time information and facilitates the analysis of this information. By processing the sensed data at a node, connected devices perceive their surroundings and understand what is going on [4] [5].This collected data enables devices to take decisions autonomously or propagates information to users in order to make the best decisions [5].

Cloud and IoT are mutually dependent on each other. IoT benefits from the virtually unlimited capabilities and resources of Cloud to reduce its technological constraints (e.g., storage, processing, and energy). Cloud can benefit from IoT by enlarging its scope to deal with objects in real world and delivering more services in a distributed and dynamic way [6]. however, integrating IoT with cloud services introduces significant security and privacy challenges. Using IoT paradigm, everything relies on the integrity of the data. This data should be secure and private as it is exchanged within the complete integrated environment of cloud facilities [7].

*Corresponding author: N.Sriram*

In the E-health environment, Cloud and IoT technologies deployed as part of medical information systems must satisfy specific important security requirements such as integrity, confidentiality, availability, and authentication, in order to protect medical data without reducing the efficiency of services [8].

## II .IOT AND CLOUD: OPPORTUNITIES AND VULNERABILITY IN EHEALTH CONTEXT

A. Iot and cloud : opportunities in the healthcare
Cloud Computing and IoT integration provides new storage, processing, scalability and networking capabilities, which play a key role in developing and maintaining smarter, connected and personalized healthcare services. The ability of auto-configuration, interoperability, self-management, intelligent interaction with other things and initiation of processes based on data and context makes the care process more efficient and cost-effective and improves the decisions of medical staff [40]. Thanks to the simplified standard communication protocol between wired and wireless medical devices [12], the networking of biomedical instruments and databases in hospitals improves the quantity and availability of diagnostic and treatment decisions [9]. IoT and Cloud technologies have also considerable implications for rural and remote clinics, providing ready access to specialist opinions [10].

Furthermore, extending medical instrumentation to the home has improved quality of life and reduced hospital readmissions [11]. Medical Body Area Networks (MBAN's) open the door for monitoring systems to operate wirelessly using low-cost wearable sensors [24].

B. Security requirements in E-health Context
Firstly the e- Health definition cited by The World Health Organization [WHO] is: "E-health is the transfer of health resources and health care by electronic means. It encompasses three main areas: The delivery of health information, for health professionals and health consumers, through the Internet and telecommunications.
To protect this health information, HIPAA (Health Insurance Portability and Accountability Act) establishes a series of security standards for the use and disclosure of "protected health information" (PHI) [30].

The Security rule focuses on administrative, technical and physical safeguards specifically as they relate to electronic PHI (ePHI). ePHI is any Protected Health Information (PHI) which is stored, accessed, or communicated electronically. The Protection of ePHI data from unauthorized access is part of the security rule.

The focus of the security rule is to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) [30, 31].

Confidentiality is the assurance that ePHI data is shared only among authorized persons or organizations. Confidentiality protection applies to data in storage, during processing, and while in transit. Integrity is the assurance that ePHI data has not been altered in an unauthorized manner while in storage, during processing, or while in transit.

Moreover, any modification of data must be known, required, documented, validated and approved. Most important to HIPAA, data integrity ensures that we can rely on data in making medical decisions. Availability is a requirement intended to assure that services of delivering, storing and processing critical ePHI data are accessible to authorized users when needed, under both routine and emergency situations.

C.IOT vulnerability in a cloud context:
We briefly describe in this section a three layers architecture that we consider in our Iot vulnerability analysis [15, 21, 27, 28, 29].

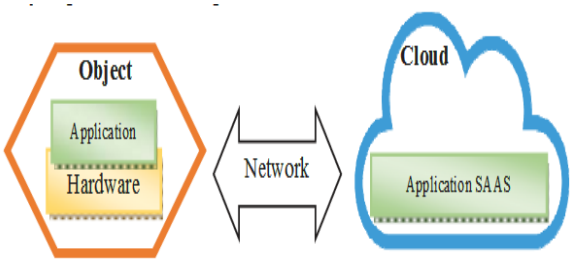


**Fig.1. Layers of IOT vulnerability in a cloud**

### 1) Hardware vulnerability:

The smart objects in the sensing domain are expected to be secured against physical attacks, both from weather and individuals perspective. Common issues in Physical Layer are:

- Physical Damage: This vulnerability concerns physical devices such as sensors, nodes and actuators which can be physically damaged by the malicious entities or by Environmental hazards. This could cause the devices to lose their functionality and become vulnerable to other risks.

•Resources constraints:
IoT devices are resources constrained. These constraints could be in terms of available computational resources, onboard memory or energy availability, etc. Devices that run out of power essentially cannot operate normally and this results in a denial of service
• Storage vulnerability:
IoT enables data to be stored in both physical devices and cloud storages. Personal data and security proprieties must been kept within an IoT device.

**2) Network vulnerability:**

•Data Interchange vulnerability:
Data exchanged via network may be a subject of DoS or gateway attacks. These attacks can shut down the transfer of data between the devices and their source. An overflow of data is sent to the device may shuts down its processes. This might be the case, when networks services are found with unnecessary exposed and available ports. Moreover, a variety of data containing vital information of the user need to be stored on un trusted cloud, which can be damaged and the data may be compromised or modified.
• Unauthorized Access:
A number of attacks are possible to healthcare devices and systems, if there is no proper authentication procedure.
•Multifarious connectivity Vulnerability:
Diversified smart objects are connected to the global interconnected network, IoT objects communicate with each other throw different types of network infrastructure including wireless, wired, private, and public networks. This cross protocol characteristic makes the IoT network vulnerable to various security problems like data integrity violation, inadequate quality-of-service (QoS), etc. 3) Application vulnerability: Due to security vulnerabilities in the application layer, the services may be damaged, used in an incorrect manner or accessed by unauthorized users. Common vulnerabilities to Application Layer are:
• Native application vulnerability:
Different IoT applications are available as an embedded application on the device or at the local network, this kind of application is denoted as native application. The classification of native applications is three: in device application, coordinator application and gateway application. The web interface used by those local devices might have some vulnerabilities including account: enumeration, insecure account credentials and lack of account suspension after a limited number of password guessing. Hackers benefits from application vulnerabilities on device nodes to install malicious root kits. Protecting specific parts of a device may be insufficient.
• Cloud applications vulnerability: In the case, that IoT applications are hosted on clouds, the devices and the applications can be access at anytime from anywhere. This eliminates limits for access, but incorporates security vulnerabilities at the same time as these cloud applications may be unsecure or may use services and resources from a untrusted cloud partner.
• Cryptographic vulnerability: Because of the low computational capability, IoT devices might avoid transport encryption or might use weak encryption methods. Therefore, communication becomes easy to discover and traceable by the malicious actors. Added to that, the mobility nature of IoT devices raises the need to develop mobility resilient security algorithms for the IoT devices.

## III. SECURITY SOLUTIONS FOR IOT IN EHEALTH CLOUD

Following are prominent security methods that have been proposed in the literature for of IoT that can be used in an Ehealth cloud domain.
These security methods were identified from the leading journals and conferences in order to present the recent and effective solutions adapted by researchers.
1) Hardware Security solutions: The architecture proposed in [16] is based on the embedded sensors of the equipment rather than using wearable sensors or Smartphone sensors to store the value of the basic health-related parameters. Cloud centric architecture is composed of a Cloud data center, which uses the XMLWeb services for secure and fast communication of information. Lui et al., has proposed authentication and access control in the IoT that fixes loopholes in device security and data integrity. In this solution, a user requests authentication to access a device and asks for permission from a “Registration Authority” (RA). RA in turn send user a question, if response is OK, the user is authenticated to access the device [25]. In [18] Hossain and Muhammad have focused on real-time health monitoring infrastructure for analyzing patients. They have presented a HealthIoT framework to monitor ECG and other health care related data using smart phones. The proposed architecture is designed around clouds. Authors have used the watermarking techniques for security of data to

be communicated. In [17] the authors deploy a file retrieval and error recovery based mechanism to detect any unauthorized data modification and corruption due to server compromise or random failures.

2) Network Security solutions: Current researches [13][12] related to IoT Cloud platform focuses on architectural design to realize a health monitoring and analysis system. For example, in [12], the authors propose a framework of IoT-Cloud using VIRTUS middleware for ehealth system. It is a publish/subscribe system using XMPP protocol. VIRTUS provides to the system a reliable, scalable and secure communication channel in order to exchange the data safely over internet and eliminate the data loss in case of poor connectivity. In [36] is proposed a new option to The Constrained Application Protocol (CoAP) [37], which works at the application layer. CoAP provides the ability to retrieve data from devices like metadata and its sensor measurements. Sometimes there is a security requirement to not retrieve raw communication data, which this protocol did not respect. In addition to the nature of the resource of constrained devices, which can be accessed by anyone on the Internet, energy consumption reduction mechanism plays a critical role. Proposed mechanism contributes to these two requirements and reduces the messages number when observing a sensor resource, which can result in energy consumption reduction and increasing lifetime of the device. In [39], a novel authentication mechanism for IoT networks have been proposed. The proposed architecture of reliable and secure healthcare solution uses an (ECC) Elliptic Curve Cryptography algorithm [38] over the CoAP protocol. The proposed authentication approach provides an efficient authentication mechanism with high security. In [19], the authors propose a new key management protocol based on collaboration to establish a secured communication channel between a highly resource constrained node and a remote entity (i.e. server). The secured channel allows the constrained node to transmit captured data while ensuring confidentiality and authentication. The protocol offloads consuming cryptographic primitives to third parties, which are not necessarily trusted. Authors in [20] describe a solution of Construction of a patient-oriented PHR system on clouds .the authors develop an improved oblivious transfer protocol to offer the possibility of communication between users and the trust authority. The principal idea is that the receiver selects the desired message under the conditions that the sender cannot know which message the receiver had choose. The proposed scheme attains the goal of protecting both the user and server privacy and security as well as provides the access for multi-users. Z. Li's propose a PKI-Like Protocol that involves encrypting the routes of nodes to their destinations and using a key for decryption and security. The data is sent along the way to and "offspring node", that then transmits the key when the node reaches the destination node [26]. In [32], is proposed a Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications. This protocol supports resource limitation of sensor nodes and the network scalability and heterogeneity. Two phase authentication allow IoT devices and the control station to authenticate each other, a secure connection is established and data is transferred securely. Certificate authority (CA) has been used to issuing certificates. After getting their own certificate, the nodes can move and change their location. CA can validate sensors identity and communicate with other entities of the network. This approach is considered as an endto-end application layer authentication approach and depends on other lower layer security features. In [35], Threshold Cryptography-based Group Authentication (TCGA) scheme for the IoT is proposed. TCGA is designed to be implemented for Wi-Fi environment and provides authenticity for all IoT devices of the group communication model. It initialize a secret session key for each group authentication. Each group has a group head, which is responsible for key generation and distributing every time when a new group member is added. The Proposed algorithm has five main modules: key distribution, key update, group credit generation, authentication listener and message decryption.

**3) Software Security solutions:**

In [33], a secure authentication scheme for IoT and cloud servers have been proposed. The schema depends on Elliptic Curve Cryptography (ECC) based algorithms, which supports better security solutions because of its small key size. This authentication protocol uses EEC for embedded devices, which use HTTP protocol. These smart devices need to be configured with TCP/IP and use cookies of HTTP to be authenticated, which is a novel approach. SEA [34], which is a Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways. The proposed architecture mainly depends on

certificate-based DTLS handshake protocol. This architecture includes three main parts: medical sensor network, which collect data from patents body or rooms for medical diagnosis. The second part is Smart e-Health Gateway that enables various system communication and acts as intermediate for MSN and the internet. The third part is BackEnd System, which receives, processes and stores collected data. The Identity Framework Management Methods proposed by A. Sardana and S.Horrow solves issues regarding the authentication of data and processes between the cloud and sub-sequential communication devices. It suggests having an Identity manager that authenticates the data and then forwards it to a Service Manager to validate the instructions of the service to be performed [23]. In [14], the authors proposed a data partitioning and scrambling method at the application layer for healthcare data, where a tiny part of the original data is used to scramble the remaining data without any cryptographic key, and the former is kept locally while the latter under extra protection is sent to cloud platforms. The proposed security mechanism is deployed at the application layer of the TCP/IP five-layer model, which can be easily used in other existing communication systems as an add-on for security.

## IV. PROPOSED ARCHITECTURE

From the literature reviewed, we can find that there is still a lot of possibility for the improvement of the security for IoT architectures in the eHealth cloud context. Most of the proposed health care IoT -cloud systems are over optimized as they generate large amounts of data, and continuously send alerts to the users and medical staff, which are of no use. The insufficient security of IoT devices may cause a damage for cloud environment by allowing the sending of incorrect data. Keeping these shortcomings a priority, we propose an IoT-cloud based development solution using distributed security strategy architecture. The proposed architecture is based on the distribution of both process and security of health information. Different security mechanisms are proposed in order to protect the different layers of the architecture. The figure 2 present the proposed components of this solution:

• For Hardware layer:

we propose using smart devices, which not only collect health data but also embed security mechanism and encrypt data before sending it to the cloud application layer. Another functionality of smart devices is to prepare the data before sending it , for example in the case of patient temperature control , the smart device does some arithmetic operations to compare the data with predefined levels and then send only the result of the operations such as (ordinary , the temperature is high .. ). The local treatment of data increases the confidentiality of the information. Moreover, the local security mechanism (denoted as SDL in the fig 2) ensure integrity and confidentiality as the patients data are coded when they cross the network.

• For Network Security: we propose a local temporary back up in the IoT environment to ensure the availability of information in case of network discharge or an attack. A Certificate authority (CA) is proposed to secure the exchange of data.

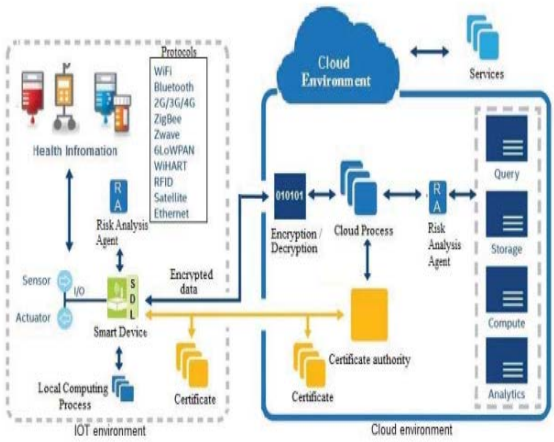


**Fig. 2: Proposed Architecture**

• For Software security:

Added to the standard mechanisms of cryptography and access control, we propose a risk-analysis agent for both cloud and IoT environment to estimate and predict risk damages and future benefits, and to learn identified new or unknown threats to IoT-cloud based eHealth systems. V. CONCLUSION We have discussed in this paper how integrating Cloud and IoT provides several benefits in the ehealth domain. We discuss also different vulnerability of Iot in a cloud context and we present recent solutions for the IoT and Cloud security proposed specially to protect the health information. We finish by giving a proposition of using a distributed security architecture in both devices and cloud application layers.

## REFERENCES

1. Bai, Y., Dai, L., Chung, S. and Devaraj, D. D.,"Access control for cloud-based eHealth

social networking: design and evaluation." Security Comm. Networks,2013.

2. Q. Duan, Y. Yan, and A. V. Vasilakos, "A survey on service-oriented network virtualization toward convergence of networking and cloud computing," IEEE Transactions on Network and Service Management, Vol. 9, No. 4, pp. 373-392, 2012.
3. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach," Future Generation Computer Systems, 2014.
4. Q. Zhou and J. Zhang, "Research prospect of Internet of Things geography," in Proceedings of the 19th International Conference on Geoinformatics. IEEE, 2011, pp. 1–5.
5. Y. Yu, J. Wang, and G. Zhou, "The exploration in the education of professionals in applied Internet of Things engineering," in Proceedings of the 4th InternationalConference on Distance Learning and Education (ICDLE) , pp. 74–77. IEEE, 2010.
6. Jiehan Zhou, Leppanen," CloudThings, A common architecture for integrating the Internet of Things with Cloud Computing", International Conference on Computer Supported Cooperative Work in Design,pp 651-657, June 2013.
7. H.Kumarage, I.Khalil, A. Alabdulatif, Z.Tari, and X. Yi, "Secure Data Analytics for Cloud-Integrated Internet of Things Applications" IEEE Cloud Computing published by the IEEE computer society March/April 2016.
8. Ma, Y., Liu, J., and Liu, W., "Security and privacy issues in electronic health network". Wuhan J. Natur. Sci. 18(6):523–529, 2013.
9. Yu, L.; Lu, Y.; Zhu, X. Smart hospital based on internet of things. J. Netw, 7, 1654–1661, 2012. [10] Mars, M. "Telemedicine and advances in urban and rural healthcare delivery in Africa." Prog. Cardiovasc. Dis., 56, 326–335, 2013.
10. Wade, V.; Soar, J.; Gray, L."Uptake of telehealth services funded by medicare in Australia." Aust. Health Rev, 38, 528–532. 2014.
11. Bazzani, M., Conzon, D., Scalera, A., Spirito, M. A., & Trainito, C. I." Enabling the IoT Paradigm in E-health Solutions through the VIRTUS Middleware. In Trust, Security and Privacy in Computing and Communications "(TrustCom), IEEE 11th International Conference on (pp. 1954-1959). 2012.
12. C. Doukas and I. Maglogiannis, "Bringing IoT and Cloud Computing towards Pervasive Healthcare," 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Palermo,, pp. 922-926, 2012.
13. S. D. Bao, Y. Lu, Y. K. Yang, C. Y. Wang, M. Chen and G. Z. Yang, "A data partitioning and scrambling method to secure cloud storage with healthcare applications," 2015 IEEE International Conference on Communications (ICC), London, pp. 478-482, 2015.
14. D. Lake, R. Milito, M. Morrow, and R. Vargheese, "Internet of Things: Architectural framework for ehealth security," Journal of ICT Standardization, River Publishing, vol. 1, 2014.
15. Gupta, P.K., Maharaj, B.T. & Malekian, R. "A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres" Multimed Tools Appl (2016).
16. Jin Wang, Hassan Abid, Sungyoung Lee, Lei Shu, and Feng Xia." A secured health care application architecture for cyber-physical systems." arXiv preprint arXiv:1201.0213, 2011.
17. Hossain MS, Muhammad G "Cloud-assisted industrial internet of things (iiot):enabled framework for health monitoring. ",Comput Netw 101:192–202,2016.
18. Abdmeziem MR, Tandjaoui D." An end-to-end secure key management protocol for e-health applications".Comput Electr Eng ,2015.
19. Chen SW, Chiang DL, Liu CH, Chen TS, Lai F1, Wang H,Wei W. "Confidentiality Protection of Digital Health Records in Cloud Computing". J Med Syst. , May 2016.
20. Subho Shankar Basu; Somanath Tripathy; Atanu Roy Chowdhury ," Design challenges and security issues in the Internet of Things", IEEE Region 10 Symposium (TENSYMP), 2015.
21. Dohr, R. Modre-Osprian, M. Drobics, D. Hayn, G.Schreier, "The Internet of Things for Ambient Assisted Living", Seventh International Conference on InformationTechnology, pp. 804-809, 2010.
22. Sardana and S. Horrow, "Identity management framework for cloud based internet of things", Proceedings of the First International Conference on Security of Internet of Things,pp. 200-203, 2012.
23. Felipe Fernandez; George C. Pallis "Opportunities and challenges of the Internet of Things for healthcare", Wireless Mobile

Communication and Healthcare (Mobihealth), EAI 4th International Conference, 2014.

**24.** Lui, Xiao, Chen. “Authentication and Access Control in the Internet of things”, 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), pp.588 – 592, 2012.

**25.** Zhihua Li et al., “Research on PKI-like Protocol for the Internet of Things”, Fifth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), pp. 915 – 918, 2013.

**26.** Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I.. “ Internet of things: Vision, applications and research challenges”, Ad Hoc Networks, 10(7), 1497-1516, 2012.

**27.** K.Sonar and H. Upadhyay, "A Survey: DDOS Attack on Internet of Things", Intl. Journal of Engineering Research and Development, vol. 10, no. 11, pp. 58-63, November 2014.

**28.** Chen, C., Yang, T., and Shih, T., “A secure medical data exchange protocol based on cloud environment.” J. Med. Syst. 38:112, 2014.

**29.** http://hipaa.yale.edu/security.

**30.** Glossary of Key Information Security Terms http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST .IR.7298r2.p df.

**31.** P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in IEEE Wireless Communications and Networking Conference (WCNC), pp. 2728-2733, 2014.

**32.** S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," Pervasive and Mobile Computing, vol. 24, pp. 210-223, 2015.

**33.** S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, et al., "SEA: a secure and efficient authentication and authorization architecture for IoTbased healthcare using smart gateways," Procedia Computer Science, vol. 52, pp. 452-459, 2015.

**34.** P. N. Mahalle, N. R. Prasad, and R. Prasad, "Threshold Cryptography-based Group Authentication (TCGA) scheme for the Internet of Things (IoT)," in Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 4th International Conference on, pp. 1-5, 2014.

**35.** R. Mietz, P. Abraham, and K. Römer, "High-level states with CoAP: Giving meaning to raw sensor values to support IoT applications," in Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP),IEEE Ninth International Conference, pp. 1-6, 2014.

**36.** Shelby, Zach, Klaus Hartke, and Carsten Bormann. The constrained application protocol (CoAP). No. RFC 7252. 2014.

**37.** H. Marzouqi, M. Al-Qutayri, and K. Salah, "Review of Elliptic Curve Cryptography processor designs," Microprocessors and Microsystems, vol. 39, pp. 97-112, 2015.

**38.** Mustafa Abdullah Azzawi, Rosilah Hassan and Khairul Azmi Abu Bakar “A Review on Internet of Things (IoT) in Healthcare” International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 20 ,pp. 10216-10221, 2016. [40] Zhanlin Ji; Xueji Zhang; Ganchev, I.; O'Droma, M., "A personalized middleware for ubiquitous mHealth services," e-Health Networking, Applications and Services (Healthcom), 2012 IEEE 14th International Conference on, pp.474,476, 10-13 Oct. 2012.

**39.** European Commission Information Society. Internet of Things Strategic Research Roadmap 2009. http://www.internet-of-things-research.eu/.