

Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications

Maria Almulhim*, Noor Zaman*

*College of Computer Sciences and IT, King Faisal University, Saudi Arabia

maria.almulhim1@gmail.com, nzaman@kfu.edu.sa

Abstract— The Internet of Things (IoT) is the collection of connected smart devices\objects through internet network. The rapid development of IoT and vast expansion of wireless technologies unfold the new chances of growth in several domains such as, Education, Transportation, Agriculture, and especially in the Healthcare sector. Introducing the IoT through healthcare applications fetch several benefits, including cost savings through lowered hospital visiting costs, health care provider costs, transportation costs, human resource costs and the insurance costs. It leads to an added advantage of improved quality care in health care. However, increasing use of the IoT services in E-health applications has led to increase the concerns of security and privacy, especially in healthcare domain. In fact, healthcare applications are prone to data breaches and widening issues in security aspects owing to increasing number of access points to sensitive data through electronic medical records, as well as the rising popularity of wearable technology. For example, of these issues, authentication of the different connected entities, energy efficiency and exchanged data confidentiality form the major concerns for users. Therefore, the successful deployment of IoT-based E-health application rely on overcome the major security concerns for the users which needs to be addressed in energy efficient way. Though a number of researches have conducted for lightweight secure authentication, there is still a great room for further research to address security challenges as well as its energy efficiency for those security authentication schemes in IoT. There is a great need to design and develop a lightweight secure authentication model, which offers significant security level against multiple attacks such as mainly: Impersonation attacks, man in the middle attack and unknown key sharing attacks for IoT base E-health domain. This research proposed a secure group-based lightweight authentication scheme for IoT based E-health applications, the proposed model will provide mutual authentication and energy efficient, and computation for healthcare IoT based applications. Which will use elliptic curve cryptography (ECC) principles that provide mentioned featured of suggested model.

Keywords— Secure, Authentication, Light weight, ECC, IoT

I. INTRODUCTION

During last few years, IoT (IoT) is rapidly gaining ground in the field of networking wireless and communications. The basic idea is the connection between heterogeneous objects such as Mobile phones, Sensors, Radio-Frequency Identification (RFID) tags, etc. Therefore, everything becomes virtual, which means that everything is readable, addressable, and locatable on the Internet. The IoT is growing in several domains such as, Education, Transportation, Agriculture, and especially in the healthcare sector [1].

Healthcare application is reflecting one of the most IoT technologies and it is named as IoT-based healthcare applications. It provides multiple of features like continuous remote monitoring of data, so patients can be monitored daily by using sensors in mobile devices such as cell phones or wearable devices. Thus, it is expected that IoT-based healthcare applications to offer multiple of benefits that include such as cost savings through lowered hospital costs, health care provider costs, transportation costs and insurance costs. Therefore, this will have led to improved quality of care and time saving for patients and hospital staff. Therefore, facilitate flexible and secure interactions between patient and healthcare providers is the main goal [2].

So, with rapid deployment of IoT this has brought a lot of challenges, issues and security and privacy concerns. Security is substantial part at lifecycle of medical information of IoT-based healthcare applications and aim to provide the secrecy of those medical data [3].

There are multiple of security issues that need to be handled are: authentication (which is the aim of our research), availability, data integrity, Confidentiality, and non-repudiation to save the data and maintain the efficiency and quality of healthcare provider services. Authentication is an important part at IoT, it enables each object at network to authenticate each other so it will let to forwarding the data to the receiver without any alternation in information [3].

In fact, healthcare applications are prone to data breaches and widening issues in security aspects owing to increasing number of access points to sensitive data through electronic medical records, as well as the rising popularity of wearable technology [1].

Though a number of researchers have discussed open issues in IoT security, there is a need for further research to address security challenges in IoT [4]. The main goal is to make security a fundamental part in design of IoT based healthcare technology for protected data transfer, use and exchange [5].

So, based on that our paper aim to propose a secure group-based lightweight authentication scheme for IoT based E-health applications, which offers high security level against multiple attacks and mutual authentication with less costs in healthcare IoT based applications.

At beginning paper, we discuss briefly about security issues of IoT based E-health applications. The reminder of this paper organized in four different sections. In section II, we present Literature review. In section III, we proposed our scheme and

explained its technique. In section IV, we have brief discussion about our expected outcomes. Finally, Section VI, we conclude with the important points of the paper.

II. RELATED WORK

At study [2], they analyse the concept and effects of IoT about establishing solves of E-health and specifying most main challenges which strict the successful deployment of IoT-based e-health applications. The new and rapid deployment of IoT technology, Big data and Cloud computing has led to change the improve mechanism of manage patients and healthcare provider in health care industry and this fetch several benefits, including: cost savings through lowered hospital visiting costs, health care provider costs, transportation costs, human resource costs and the insurance costs. It leads to an added advantage of improved quality care in health care. So, to reach a broad scale of adoption of success IoT base E-health they need to address the barriers and issues such as: security and privacy challenges. With the rapid gaining ground in the field of networking wireless, communications and technologies, the use of wearables devices has been increasing and become more useful for patients.

Therefore, the insurance of security and privacy of user is the most important key to have useful use of and IoT base E-health applications. Moreover, this need to use high security protocols, which monitor access and identify identity. So, based on that at this study they did a review about some solutions to improve present IoT base E-health applications.

At study [3], they present last security threads and challenges at E-health systems and they discuss about how to be addressed that issues by developers and designers in future to face that attacks that came from wide using of new IoT technologies.

E-health applications are one of the main important factors that facilitate patient's life by providing multiple of broad services. The new and rapid deployment of E-health technology led to costly security threats. Therefore, they discover the reasons and concerns. After that, they present the last security threads with the suitable solutions to reduce these threads.

Then, they specify the future security and privacy issues that may happen and how to deal with them when use E-health applications.

Later, they display some of security and privacy issues that related to E-health applications: Biometrics, Cloud computing, social networks, IoT, Smart health and smart cities. These mentioned issues are out of scope of this study and they plan to analyse them at their future works.

At study [6], they proposed narrowband IoT (NB-IoT), its preferably utilized in healthcare areas because it has low energy needs. It had been proposed several of suggestions to apply NB-IoT in the healthcare areas. In addition, NB-IoT is suitable with cellular platforms because it has been unified, for that reason it's a good option to be utilize in E-health applications. However, the security concerns are the major barrier for NB-IoT. However, it can be a good option for E-

health applications if they are handling these challenges correctly. At this study, they proposed these current challenges at NB-IoT and proposed suitable solutions.

One of the major challenges are lack of provide service in real time and bandwidth inability due to unable of monitoring through the delay. This will not be useful in E-health applications for that reason we cannot depend on NB-IoT

To deal with issues related to real-time it can solve by using: IPv6 over WPAN (6LoWPAN) and constrained application protocol (CoAP). In addition, they can utilize efficient sharing resource algorithms to addressed real-time issues. It is predicted that NB-IoT will be portion of new E-health applications.

At study [7], they analyst the benefits, threat models, security needs of security and privacy in IoT-based health field. In addition, they suggest security model, which collaborate to reduce security issues, and how take benefits of multiple technologies, like: wearables, big data and so on.

They also handling different policies that related to IoT-based health and offers methods of for incoming research for open challenges in this field.

This study present multiple fields of technologies of IoT-based healthcare and some of their architectures which backing and facilitate access, transfer and receive of medical data. Furthermore, this study offers deep studies about how IoT-based healthcare application handle many medical services of patients. So, it's predicted that the outcomes of this survey are helpful for authors, health providers and researchers at field of IoT-based health applications.

At study [8], this study offers for these IoT nodes a security framework through cloud system virtual network. One of the top flaws in IoT cloud networks is problems of their nodes when utilized through cloud system virtual network. These nodes can communicate with each other through virtual network and this require observation by cloud service provider (CSP). CSP requires to be careful that these the malicious node cannot separate through network.

They suggest secure key management protocol among set of users and CSP, which have IoT nodes that utilized balanced incomplete block design (BIBD) model. Then, they prepare lightweight cryptographic mechanism that has valid key exchange protocol to create safe end-to-end communication through these nodes. After that, they utilized multiple measurements to measure flexibility and efficiency of the distribution.

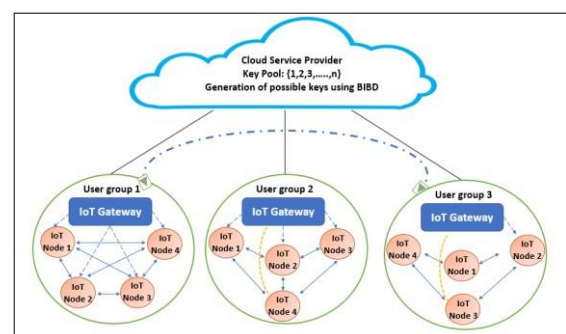


Figure 1. Balanced incomplete block design (BIBD) model [8]

At their security analysis step, they utilized Diffie-Hellman algorithm, which provide several of advantages to their work, such as low consumption of energy, strong and lightweight. Therefore, based on their security analysis and performance estimation this confirm that they are one of the main improvements of these nodes against security threads.

In future, they are planning to display inside cloud network a complete communication through multiple IoT nodes. Also, to expand and apply this protocol in hardware to estimate their efficiency and flexibility against multiple attacks.

The authors in [9], discusses the main issues that happen today, containing features and hardness, as well as oncoming to circumvent the issues of use and combine devices of Internet of Things in healthcare applications. They show this discussion in the context of the REMOA project, which provide a good solve for monitoring home for patients who have inveterate disease. There are multiple of applications for IoT; that include healthcare applications, so this is the main part of their paper.

REMOA1: project that provide a good solve for monitoring home for patients who have inveterate disease. This project also includes the styling and execute of a healthcare faithful middleware. The project by use middleware gather information from many sensors, which supply security that required in Internet of Things for healthcare. The monitoring done by linked wireless technology. There are some of the impendence have more focused due to of the troubles that effect on systems. Moreover, connection and interception issues still exist and the absence of any authentication service infrastructure for sending information is security holes, which request to solve in this project.

At this paper [10], they offer a new scheme of lightweight authentication for an E-health application. This scheme allows authenticate of both of (BS) sensors and the Base Station to secure the gathering of health-related data. Their scheme utilizes Keyed-Hash message authentication (HMAC) and nonces to make sure the integrity of authentication exchanges. Furthermore, it offers authentication with low consumption of energy, and it end with agreement of a session key between (BS) sensors and the Base Station. They make security analysis and performance to evaluate their scheme. The gained results present that their scheme maintain energy. In addition, it is resistant against multiple types of attacks. An authentication aspect at E-health applications is one of the major important challenges that should be solved efficiently. An authentication scheme avoids any wrong health-related data transferring by a malicious node.

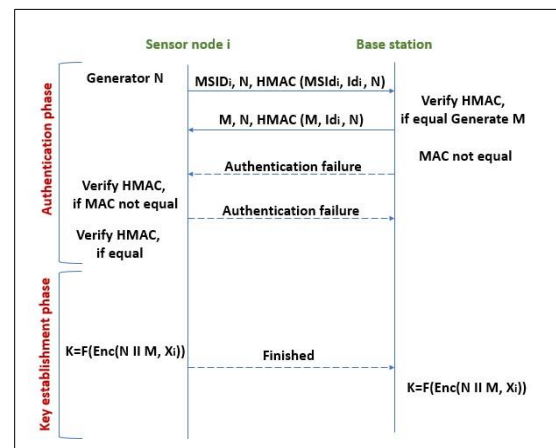


Figure 2. Lightweight authentication scheme [10]

As a future work, they plan to test their verification protocol in a real deployment to get extra precise study analysis on execution time and memory consumption.

This proposal [11] is to offer a set of cryptographic SIM card and security techniques to authenticate, sign and encrypt the medical devices communications. The initial tests presents decrease of the handover process time, by remove the steps of simplifying and processing the MIPv6 protocol. In addition to increase, the communications of security in that done by NFC (Near field communication) devices that improve with the inclusion of SIM card cryptographic.

This paper aims to fix the issues that show in the technologies that let IoT, to provide a secure, fixed and strong technology to allow the IoT might become fact in healthcare areas. For that proposal, on one side for RFID/NFC, they involve cryptographic SIM card to backing security and on the other side, for 6LoWPAN, they have evolved a mobility protocol, which is rely on the architecture to backing IoT. Thus, they specify collection of proposals to solve the challenges that in the Internet of things integration in medical environments.

As future work, on one side, they plan to take the consumption of power of the 6LoWPAN sensors than make analyse to evaluate whether the entry of the mobility protocols hold the concept of low consumption of power from LoWPAN. From other side, they will enter algorithms for find out symptoms in the architecture that implement health knowledge and chronobiology algorithms. Eventually, they are planning to merge the standard CEN/ISO 13606 for Electronic Health Record to exchange information and export medical information between patient's residence and hospital.

In this paper [12], they discuss several e-health applications of IoT, including issues of security and privacy, remote monitoring for elderly and sleep disorders, which linked with

data and electronic medical records. One of the most substantial issues in e-health applications is security of information and monitor entry for E-health data of patient to save patient's privacy and to avoid the non-ethical use of this information.

Data transfer through the channels of wireless communication also growing the weakness due to of the shared and open features of wireless networks. The information in the wireless channel is risky to hearer and assailant that can misapply of information. The (HIPAA) health insurance portability accountability act offers multiple for security and privacy issues.

This paper [13] explains the architecture design of the security and privacy of sensitive healthcare data. They suggested architecture will utilize context of the Remote Patient Monitoring for validation. Specially, a system with links of unlock wireless, shared data and mobile users will increase the hardness of security' system. Multiple parts of privacy are built to gather, store and access the private information of patient. The basic knowledge system uses an ontology approach. While security and encryption of hardware of the transfer information is needed, this located out of the limits of the present paper.

Authors offer the MEDiSN system for monitoring patient in hospital areas. The authors suggest techniques of encryption of privacy and data security. The current BUTLER project, let the evolved of secure, sophisticated life helpful applications, which can also handle eHealth cases. The authors also suggest authentication user and encryption data, as well as other security measures. However, the team plan to handle encryption of the send data and any other possible security issues in future work.

This paper [14], present the Adaptive Security for Smart IoT in eHealth (ASSET) project evolved risk-based adaptive security ways and techniques for IoT app based E-health. This paper presents the setting of tests for adaptive security for the IoT that utilize present commercial off-the-shelf software and products of unlock resource.

Furthermore, the paper discusses the authentication of the setting by the education of the effect of antenna orientation on power consuming. For this reason, they add rating approach of the power consuming n, which utilize the Holt-Winters guess process, had evolved. This is helpful when explore lightweight security solves that will be portion of the ASSET project.

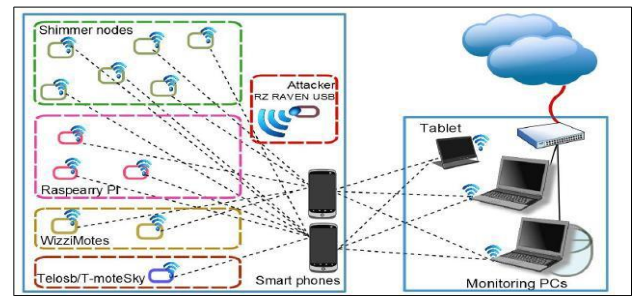


Figure 3. ASSET Project [14]

In the future, they will use the testbed presented hereby to estimate the performance of consume power of security algorithm, communication costs and hardness.

This paper [15], offer the present research of IoT in E-health that concentrate in the parts of security. Additionally, research of future works and manufacturing opinion are present specially, the works produce some prudence to the formation of this work to help extra in find out future research of security fields that centring in IoT of E-health. In addition, this paper inserts more fields to look which are network and protocol features.

Smart Health-NDNoT show the efforts of Named Data Networking (NDN) that guarantee information security rather than link security. UT-GATE plans the parts of security particularly in implement a gateway and network architecture. Fault Tolerance project concentrates on network architecture, intelligent system and real time. This work presents extra feature that are network and protocol. Some works may present their security protocols or work on existing protocols.

This paper proposed a broad variety of potential future works both from industries and academic researches, which led to the secure, solve of E-health IoT output in future.

At this study [16], they show a security framework which implement adaptive security contexts to correctly monitor needed data to prevent tackle the challenge in distributed IoT systems. The suggested solve can reach responsibility and track propagation of information, containing services, devices and parties who have legal liability and responsibility.

The suggested security context must be integrating within the entire information flow since the security hardness is similar to the lowest flow link. If the relation between the device and the gateway is exposed, the data will be compromised even if the cloud of the security is powerful. The major concept of their framework security Context is the build of security context connected with every source, which in this scenario, is a part of private E-health data. When a part of data is build, the related security context must be produced automatically.

In this article [17], they evaluate schemes of lightweight and escrow-free, assist their security and performance in terms

of energy consumption and handling time in the TelosB platform so they are planning to specify AKA solve appropriate for the IoT cases. Besides proving and show that some effective schemes are actually flawed, they present that the set of SMQV (strengthened-Menezes-Qu-Vanstone) with implicit certificates produce lightweight and a private AKA protocols. Sensor nodes usually have a restricted number of sources. Therefore, the major build aims of WSN-oriented security schemes is to improve network usage and processing, enabling sensors to save power and this led to expand the life of network.

Actually, even though they were able to specify AKA schemes that are possibly more efficient than SMQV, they show sharp security errors, which mean that introduce huge refinements over SMQV is not relaxed mission.

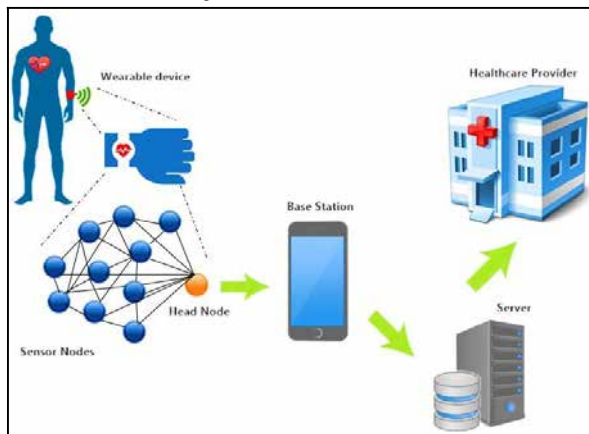


Figure 4. Proposed Scheme

In this paper [18], they offer the first completely scheme execution of two-way authentication security for the IoT (IoT) that depend on current Internet ethics, precisely the Datagram Transport Layer Security (DTLS) protocol. The verification is executing through a completely authentic DTLS handshake and rely on a swap of X.509 certificates that including RSA keys.

Their suggested security module is depending on RSA, which is the most broadly utilized public key cryptography algorithm. It is built to run through typical communication stacks that provide UDP/IPv6 networking for Low Power

Wireless Personal Area Networks (6LoWPAN). Their execution of DTLS is show in the context of a system architecture and the protocols possibility is additional established over wide assist on a hardware platform that proper for the IoT. The wide assist, depend on actual IoT systems, present that their suggested architecture offers secrecy and validity, message integrity, with low energy, end-to-end latency and memory costs. This indicate that DTLS is a practical safety solve for the developing IoT.

They are planning in future work to implement these mechanisms to DTLS with an Authenticated Encryption with Associated Data (AEAD) mode of processes to reach the minimum in network costs. Another concentration will be they introduce of extra forced nodes with no a TPM in their architecture.

III. PROPOSED SCHEME

We shall propose a lightweight authentication scheme for E-health applications, which authenticates each IoT device and builds secure channels among the sensor nodes and Base Station (BS). So that the scheme will provide authentication of individual nodes and facilitate session key agreement among BS and sensor nodes within real time constraints. The proposed scheme will be evaluated against multiple attack scenarios, namely: Impersonation attacks, man in the middle attack and unknown key sharing attacks for IoT domain.

In order to save energy, cost we plan to apply group-based authentication model, which allows all nodes to forward respective data to group head that in turn, communicates with the base station. This node may be selected based on the distance to the base station to reduce the communication cost and settle group key within a desired time limit as illustrated in Figure number 4.

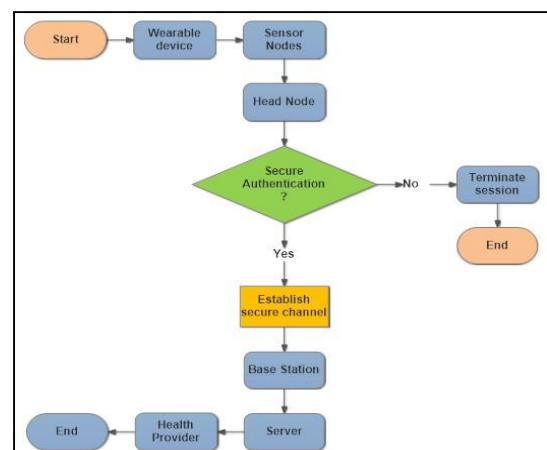


Figure 5. Flow chart of proposed scheme

Figure number five illustrate the flow of propose secure lightweight authentication scheme, where process will be initiated from the patient side and the node registration process will be started through the head node with base station. This registration mechanism will reduce the iterations of registration process on individual basis and also reduce the distance, which results energy efficiency of the scheme as well as secure communication. The IoT based objects will collect the medical records\data through wearable devices and then transfer their data to the group head node. Finally, the group head will forward the medical records\data to the server through base station.

IV. DISCUSSION

This paper presents lightweight authentication scheme for the benefit of healthcare providers and patients. In sum, the expected results of this paper are to design lightweight authentication scheme mainly using mainly ECC principles for IoT based E-health applications. To develop an authentication scheme with small key size providing comparable level of security, introduces group based authentication scheme\model for secure data transmission from IoT nodes to the base station for IoT based E-health application and provide efficient, lightweight and secure authentication scheme for IoT based E-health applications, as illustrated with the section entitled proposed scheme.

V. CONCLUSION

It's well known that the future of services of healthcare providers will rely on IoT based E-health applications. Today, IoT based E-health applications have been used widely due to their multiple of features which led to considerable cost savings through lowered hospital costs, health care provider costs, transportation costs and insurance costs. There is an added advantage of improved quality of care and time saving for patients and hospital staff. However, this widely used of E-health services open doors for security issues and increase gaps due to increase number of users' access points that can be exploited by attackers and this led to threaten the security and privacy of medical data. The main goal is to make security a fundamental part in design of IoT based healthcare technology for protected data transfer, use and exchange through the design of a Lightweight secure group based authentication scheme for IoT based E-health applications.

ACKNOWLEDGMENT

We acknowledge with thanks and appreciations to College of Computer Sciences & IT, King Faisal University, Saudi Arabia for providing this precious opportunity and environment to complete this research.

REFERENCES

- [1] Suhardi, and Alfian Ramadhan. "A Survey of Security Aspects for IoT in Healthcare." Lecture Notes in Electrical Engineering Information Science and Applications (ICISA) 2016, 2016, pp. 1237–1247., doi:10.1007/978-981-10-0557-2_117 12
- [2] Maksimović M., Vujović V. (2017) Internet of Things Based E-health Systems: Ideas, Expectations and Concerns. In: Khan S., Zomaya A., Abbas A. (eds) Handbook of Large-Scale Distributed Computing in Smart Healthcare. Scalable Computing and Communications. Springer, Cham
- [3] Zeadally, S., Isaac, J.T. & Baig, Z. J Med Syst (2016) 40: 263. <https://doi.org/10.1007/s10916-016-0597-z>
- [4] Hossain, Md. Mahmud, et al. "Towards an Analysis of Security Issues, Challenges, and Open Problems in the IoT." 2015 IEEE World Congress on Services, 2015, doi:10.1109/services.2015.12 3
- [5] Williams, Patricia A H, and Vincent Mccauley. "Always connected: The security challenges of the healthcare IoT." 2016 IEEE 3rd World Forum on IoT (WF-IoT), 2016, doi:10.1109/wf-iot.2016.7845455 2
- [6] Anand, Sharath, and Sudhir K. Routray. "Issues and challenges in healthcare narrowband IoT." 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), 2017, doi:10.1109/iciict.2017.7975247.

- [7] Islam, S. M., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. (2015). The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access, 3, 678-708. doi:10.1109/access.2015.2437951
- [8] Moharana, S. R., Jha, V. K., Satpathy, A., Addya, S. K., Turuk, A. K., & Majhi, B. (2017). Secure key-distribution in IoT cloud networks. 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS). doi:10.1109/ssps.2017.8071591
- [9] Tarouco, Liane Margarida Rockenbach, et al. "IoT in healthcare: Interoperability and security issues." 2012 IEEE International Conference on Communications (ICC), 2012, doi:10.1109/icc.2012.6364830
- [10] Khemissa, Hamza, and Djamel Tandjaoui. "A Lightweight Authentication Scheme for E-Health Applications in the Context of IoT." 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015, doi:10.1109/ngmast.2015.316
- [11] Valera, Antonio J. Jara, et al. "An Architecture Based on IoT to Support Mobility and Security in Medical Environments." 2010 7th IEEE Consumer Communications and Networking Conference, 2010, doi:10.1109/ccnc.2010.5421661
- [12] Olga Boric-Lubecke, et al. "E-Healthcare: Remote monitoring, privacy, and security." 10 July 2014. 10.1109/MWSYM.2014.6848602
- [13] Ivascu, Todor, et al. "Considerations towards security and privacy in IoT based eHealth applications." 2016 IEEE 14th International Symposium on Intelligent Systems and Informatics (SISY), 2016, doi:10.1109/sisy.2016.7601512
- [14] Berhanu, Yared, et al. "A testbed for adaptive security for IoT in eHealth." Proceedings of the International Workshop on Adaptive Security -ASPI 13, 2013, doi:10.1145/2523501.2523506
- [15] Suhardi, and Alfian Ramadhan. "A Survey of Security Aspects for IoT in Healthcare." Lecture Notes in Electrical Engineering Information Science and Applications (ICISA) 2016, 2016, pp. 1237–1247., doi:10.1007/978-981-10-0557-2_11712
- [16] Sangpetch, Orathai, and Akkarit Sangpetch. "Security Context Framework for Distributed Healthcare IoT Platform." Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering IoT Technologies for HealthCare, 2016, pp. 71–76., doi:10.1007/978-3-319-51234-1_11
- [17] Jr., Marcos A. Simplicio, et al. "Lightweight and escrow-Less authenticated key agreement for the IoT." Computer Communications, vol. 98, 2017, pp. 43–51., doi:10.1016/j.comcom.2016.05.002 16
- [18] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "Dtls based security and two-way authentication for the IoT," Ad Hoc Networks, vol. 11, no. 8, pp. 2710–2723, 2013



Maria Almulhim received the B.A. degree in Computer science from the College of Computer Science and Information Technology for girl in Hofuf, King Faisal University in 2012. Currently, study Master in computer science at the College of Computer Science and Information Technology, King Faisal University, Saudi Arabia. Current job, work as Application Analysis in National Guard and health affairs in Hofuf, Saudi Arabia.

Her areas of interest include Software Engineering, Mobile Application Programming, Web Development, and Network Management.



Dr. Noor Zaman acquired his degree in Engineering in 1998, and Master's in Computer Sciences at the University of Agriculture at Faisalabad in 2000. His academic achievements further extended with PhD in Information Technology at University Technology Petronas (UTP) Malaysia. He has vast experience of 17 years in the field of teaching and research. He is currently working as A. Professor

at College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia since 2008. He has contributed well in King Faisal University for achieving ABET Accreditation twice, by working as an active member and Coordinator for Accreditation and Quality cell for more than 09 years. He takes care of versatile operations including teaching, research activities, leading ERP projects, IT consultancy and IT management. He headed the department of IT, and administered the prometric center in the ILMA University formerly Institute of Business and Technology (BIZTEK), in Karachi Pakistan. He has worked as a consultant for Network and Server Management remotely in Apex Canada USA base Software house and call center. Dr. Noor Zaman has authored several research papers in indexed journals\international conferences, and edited seven international reputed Computer Science area books, has many publications to his credit. He is an associate Editor, Regional Editor, Program Committee, Keynote Speaker and reviewer for reputed international journals and conferences around the world. He has completed several international research grants funded by different bodies and currently involved in different courtiers for research grants. His areas of interest include Wireless Sensor Network (WSN), Internet of Things IoT, Security, Mobile Application, Ad hoc Networks, Cloud Computing, Big Data, Mobile Computing, and Communication and Software Engineering.