International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

A Secure Scheme for Trust Attribute Based Lightweight Authentication (TALA) in IoT Healthcare Environment

K. Vijayakumar, Vijay Bhanu .S

Abstract: ***Currently lot of patients is rising every day in different parts of our world. A wide range of transformation is happened in healthcare environment. Definitely Body sensor network is vital technology in healthcare environment which is used for studying purpose that functioning on IoT. Lot of Health monitoring system can be existing in environmental then operational damages. This kind of system cannot be guaranteed the patient data for end to end trust. Various existing system performance is poor for energy consumption as well as latency then communication overhead. In this paper, proposed secure scheme for Trust Attribute based Lightweight Authentication (TALA) for IoT Health Care which provides the security from IoT application. The accuracy, the transmission overhead also reduced and limited latency is achieved by the proposed system.***

Keywords : Trust based protocol, Body sensor Node, Healthcare, IoT, Medical devices.

I. INTRODUCTION

The advancement in communication technologies as well as information has opened the door for innovations in many aspects of daily life. Evolving technology called Internet of Things (IoT) which is helped equally practitioners then researchers can innovate the design solutions in different contexts, specifically in healthcare [1]. An IoT devices application is vast amount of healthcare system, estimated as accounting for over 30% of its application in all fields. Fast growth of mobile based applications, cloud computing then wearable devices which facilitates transformation of IoT role in traditional approach for healthcare to smart then personalized based healthcare. Healthcare system which enable the IoT which monitor the various parameters in medical like glucose levels, blood pressure (BP) then body temperature with computer networks, smart sensors then remote servers etc [2]. This kind of system can provide the basic treatment in healthcare that can be helpful specially used in communities or homes.

IoT is become the future so, the healthcare communities can accept the real fact.Also understand the streamlining then digitalizing the health data sharing which allow them to regain the efficiency as well as significant result of cost saving.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
K. Vijayakumar*, Department of computer science and Engineering, Annamalai University, Tamil Nadu, India. kmk.vijay@gmail.com
Dr. S. Vijay Bhanu, Department of Computer science and Engineering, Annamalai University, Tamil Nadu, India.,Vbanu22@yahoo.in

Various security actions are used for providers as well as manufacturer in IoT devices which include encryption as well as secure boot is conducted. Secure boot in the sense the device can be turned on, there is no modification among configurations [3].

There is drastic changes in medical devices of traditional unconnected equipment to reprogrammable devices wirelessly. Emerging medical IoT system have lot of advancement which include mobile phone connected to the devices. Basically, medical iot system which is comprise the health monitoring devices .Parameter for patients health can be monitored remotely by using back end system. Then the monitored data can be analyzed by back end system which provides feedback to the clinical staff. These kind of feedback helps the doctors to determine the current health status of the patient as well as take immediate action in term of patient is critical stage.

Health parameters are monitored by using medical devices. There some devices which is available for substitute the move like smart watches as well as mobile phones [4]. By the way, it can be considered as important one to record the dataset to the devices which comprises the patients health records. This will be useful for healthcare hospitals, clinics like tat. Medical IoT system setup which is sophisticated for various kind of mechanism and the systems like smart sensors, medical equipment, big data, network gateways, clinical information systems, cloud computing etc. that can be cooperate to control the healthcare environment.

The IoT-based healthcare sector is experiencing tremendous growth. The use of IoT devices and sensors in the medical sector forms the basis of the e-health system. People use these devices to monitor their daily health statistics. Simultaneously, the devices use transmission networks to send/receive the health-related data of patients. This results in a potential threat by hackers. Hence, it becomes necessary to completely secure the IoT-based healthcare system.

The organization of paper is discussed below then this work aims to improve the medical data transmission security also encryption scheme which is highly secured the healthcare system. The paper is organized by five sections which include this section. Section 2 presents the various existing works related to security oriented in healthcare system; Section 3 discussed about the proposed model and its algorithms; Section 4 discuss the experimental results discussions, finally Section 5 summarizes as conclusions.

II. RELATED WORKS

Currently, most of the projects and researches related to healthcare system is proposed that aims to provide regularly monitor the patient status, in clinic, in ambulatory then monitoring open environment like athlete health monitoring. This kind of research is popular in healthcare system by using body sensor networks.

Cifuentes, Y., et al. [5], presented the security vulnerabilities analysis then using mobile medical apps detecting the risk factors. Based on standard risk factor, this kind of apps is categorized by diagnostic support, education, remote monitoring, treatment support, awareness, medical information then training finally communication between workers in healthcare. There are eight kind of security vulnerabilities then ten types of risks factors are detected by World Health Organization (OWASP) mobile security project in 2014 is analyzed.

Healthcare system using Wireless Sensor Networks (WSN) which increases the status everyday to provide the health advice, everyday life living habitat for human beings. Though, Healthcare application which is based on WSN that faces the security and privacy related issues. WSN based healthcare applications have security considerations as well as susceptible attacks are the challenging problems. The author proposed the WSN based healthcare application for Privacy preserving scheme which utilize the secret sharing scheme, multipath routing as well as hashing principles. The healthcare data is collected from the WSN which split the components. Furthermore, each component can be computed the hash value by using hash technique. Hash value changes can be detected by message changes. Then the components can be moved to server by using multihop routing. This paper provides the new approach to validate the extensive simulations. The result shows the multihop routing for secret splitting which helps to achieve healthcare system based on WSN to privacy preserving [6].

Iot provide lot of benefits which is able to monitor the patients very closely then using data analytics in healthcare. For medical device integration in IoT which focus on customer end like blood pressure cuffs, glucose meters then other devices can be designed for recording the vital sign of patient data. It enables the healthcare providers which collect the information automatically then decision support rule is applied for early intervention of treatment process is allowed. Unfortunately, Medical Company does not consider the security risk which connects to internet. There is chance for Zero day exploits the device which injures anyone or kill anyone without detecting. Medical devices are rise for hackable to force the FDA which guide the formal issue for how medical devices handle the report which is generated by cyber vulnerabilities. This article provides the IoT role in healthcare, attacks, security issues, vulnerabilities then its solutions [7].

MIot is Medical Internet of Things which plays the important role to improve the care, safety, health of people after showing up. Instead of going to hospital, the patients related information can be monitored simultaneously then remotely in real time, Then it can be processed as well as moved to data center like cloud storage that greatly increase the cost performance, efficiency then healthcare convenience can be increased. Vast amount of data can be handled in MIoT device which grows exponentially that means sensitive data have higher exposure. MIoT devices collect the data for security as well as privacy during the data moved to cloud or stored, that can be unsolved major concerns. This articles provides the privacy as well as security requirement which related to MIoT data flow. Additionally, Existing study for security as well as privacy issues which is open challenges together for research in future works [8].

Razzaq, M. A., et al. [9], illustrate the fused security approach which is based on steganography, encryption as well as watermarking techniques. Mainly decompose with three stages namely (1) Cover image is encrypted by using XOR operations, (2) by using least significant bits(LSBs) for doing embedded process for generate the stegno image, (3) Stegnoimage get watermarking using both spatial as well as frequency domains. The results shows the proposed approach is secured and very much efficient one.

Presently, wireless body area networks (WBANs) systems is adopted by cloud computing technology which is defeated the limitations by using power, scalability, computing as well as management. The combination of cc technology and WBANs system is sensor-cloud infrastructure (S-CI), which is aided by healthcare domain by using real time monitoring the patients as well as diseases diagnosis earlier. Thus, S-CI distributed environment have new threats which is related to data privacy as well as security for patients.

Isma Masood et al, evaluate the technique for S-CI patient security as well as data privacy. Categorized the existing system namely attribute-based encryption, hybrid encryption, multibiometric key generation, Number Theory Research Unit, Dynamic Probability Packet Marking, pairwise key establishment, Priority-Based Data Forwarding techniques, chaotic maps, Tri-Mode Algorithm, then hash functions, based on their applications. The framework can be build up six steps based on the attributes of patient physiological parameters (PPPs) which is S-CI security as well as privacy: (1) preliminaries selection; (2) system entities selection; (3) technique selection; (4) PPPs accessing; (5) security analyzing; and (6) performance estimation. Now, discussing as well as identifying PPPs utilization which is provides the performance of research evolution. At last conclude with open challenges for future direction in this research domain [10].

III. REVIEW METHODOLOGY

Security is the most basic part of the framework. Alternate point of individuals which is based on the security as well as it can be characterized with multiple points of view. As a rule, security idea is well being of the framework all in all. Presently, the correspondence in sensor organize applications (like BSN) in medicinal services are for the most part remote in nature. So, the requirements of the system in two forms: one is authentication and another one is availability.

SR1: Authentication - The patient-related data sender must be authenticated, as well as data injection from outside the WBAN which was prevented.

SR2: Availability - The data which is related to patient that should be accessible still denial-of-service (DoS) attacks.

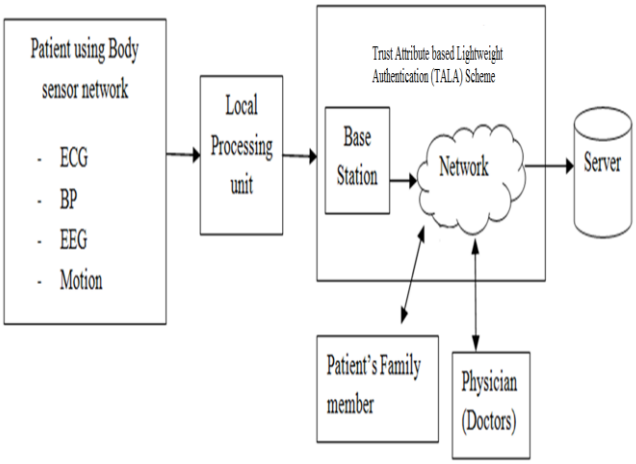

Figure 1: Proposed work flow

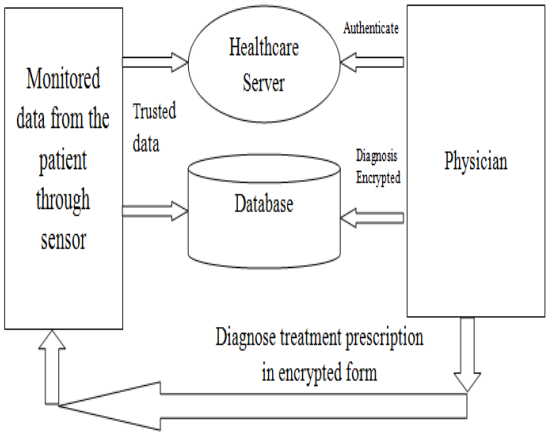

Figure 2: Trust Attribute based Lightweight Authentication (TALA) Architecture

In IoT trust valuation plays a critical role. The proficiency of the trust, valuation process is controlled by trust derivation, as it regulates the performance of network and communication overhead due to limited latency and high accuracy. In this paper, proposed secure scheme for Trust Attribute based Lightweight Authentication (TALA) for IoT Health Care which provides the security from IoT application. This works performs only the authorized doctors or experts who is access the information about the patient securely.

Body sensor network unit: Body sensor network is shown in above figure 1. In BSN system, wearable sensor is placed on patients body. Each sensor checks out the biological changes in body by using the sensor like blood pressure as well as ECG. Sensor percepts the physical body parameter which inform the action that can be send to LPU.

Local processing unit (LPU): Local Processing unit namely smart phone, PDA, embedded Kit or personal computer. It is one of the router that interconnect BSN node as well as BSN sever. LPU perform like router between BSN node and BSN server. It is used by internet through Ethernet part or Internet Dougal or GSM kit. Simultaneously monitor the patients every 10 sec physical parameters as well as stored it BSN server side.

Body sensor network server: When data from LPU the BSN server is stored in Database then it can be analyzed with standard physical data. Periodically update the data into database, if any deviation is find out that can be compared with standard data then it can be checked with database to find the patients doctors as well as relatives number to send the emergency message via internet.

Trust Attribute based Lightweight Authentication (TALA): The main aim of the study is to provide security as well as the trust in IoT system. The system security is ensured by user authentication as well as data encryption. This kind of method which record the sensor values as its parameters. The data which is recorded from the sensor in health care kit. This value is accessible by authenticated user only. The figure 2 shows the architecture of TALA.

The data which is monitored from the patient's body through ECG, BP, EEG, motion are the attributes to be considered and then, the data which is stored in the server database. Generally, the user can be validated through authentication which involves the credentials. This kind of communication is done from human to machine only. But in IoT, Communication is take places between machines to machine only which ensure the machine get authenticated by accessing the data. Machine to human communication is easy one for authentication but vulnerable attacks take place in secure communication. The two major criteria to be consider here while selecting the algorithm for authentication. Initially, the algorithm must be lightweight then it can be less computational overhead.

The proposed Trust Attribute based Lightweight Authentication scheme contains of four algorithms: System_Setup(Setup), Key_Generation(KeyGen), Encryption(Encypt) then Decryption(Decrypt).

Setup. Security parameter λ is taken as input, then which selects the tuple (p,t,r,w,d,q,m_{max}) that satisfies the following conditions.

1. Consider, elements are taken as positive integers.
2. The elements p and t which is co-prime.
3. The m_{max} element denote the plaintext maximum length

$$m_{max} < t,\ m_{max} + wrt < p$$

Let, the number of dimensions 'd' as well as the number of public key vectors 'q', respectively. The system returns the parameter params=(p,t,r,w,d,q, m_{max}).

KeyGen. System parameters 'params' is taken as input, then it generates a public and private keys pair(PK,SK) is follows.

Step1: Choose randomly a d-dimensional vector $(k_1, \ldots\ldots, k_d)$, such that $k_i \epsilon \{1, \ldots, p-1\}$ where i =1,2,…,d. At least, there is one k_i which satisfies $\gcd(k_i, p) = 1$. For the simplicity, let $\gcd(k_p, d) = 1$ and find the inverse $k^{-1}{}_d \ modulo\ p$.

Step2: A 'PK' public key which consists of 'q' public key vectors 'pk', such that $pk_i = (pk_{j,1}, \ldots, pk_{j,d})$. Where, j=1,2,…,q. The first elements 'd−1' of pk_j are sampled uniformly from {1,…,p−1}, while computing $pk_{j,d}$ in two cases below.

For j=1 is computing by $pk_{1,d}$ as

$$pk_{1,d} = k^{-1}{}_d(1 - (k_1 pk_{1,1} + \cdots + k_{d-1} pk_{1,d-1}))$$

For 2≤j≤q, chooses randomly $r_j \in \{0, \ldots r\}$ then calculates

$$pk_{j,d} = k^{-1}{}_d(pk_{j-1,d} + r_j t - (k_1 pk_{j,1} + \cdots + k_{d-1} pk_{j,,d-1}))$$

Let (PK,SK) is public and private key pair of ({pk_1,…,pk_q},(k_1,…,k_d)) and return (PK,SK). Note that two integers are used for all additions, subtractions and multiplication which is followed by the modulo operation with p.

Encryption

Encrypt. Let user's public key is PK={pk_1,…,pk_q}. A message 'm' is encrypted, such that m≤m_{max}, it computes as follows.

Step1: select randomly an integer j, where 2≤j≤q, set C=($pk_{j,1}$,…,$pk_{j,d}$) then α=$pk_{j-1,d}$.

Step2: select randomly an integer j again, where 2≤j≤q, then compute C=C+pk_j, α=α+pk_{j-1},d(mod p). Repeatedly using step for w−1 times. Note that, the 'j' value can be repeated in different selections.

Step3: Calculate then return C=C+(m−α)pk_1(mod p) ciphertext.

Decryption

Decrypt. Let ciphertext C=(c_1,…,c_d) is generated by using the public key PK=(pk_1,…,pk_q). To decrypt C by using the private key SK=(k_1…,k_d), compute

$$x = k_1c_1 + \cdots + k_dc_d(\text{mod } p),$$
$$m = x(\text{mod } t).$$

Attribute Key. To select a random γ, the secret key is β, α, ε, The 'AK' is Attribute Key and the 'D' is Decrypt.

$$AK = (D = g^{(\alpha+\gamma)/\beta}$$
$$D_1 = g^{\gamma} h^{\varepsilon}, D_2 = g^{\varepsilon},$$
$$D_3 = g^{1/\varphi}, D_4 = g^{\varphi\alpha}$$
$$D_5 = w^{\varphi\alpha}, \{\widetilde{D_j} = g^{\gamma} H_1(j)^{r_j},$$
$$\widetilde{D_j}' = g^{r_j}\}_{j \in s}$$

A. **Existing Methods for Comparison**

1. Hierarchical Attribute-Based Encryption (HABE) [11]. The fine grained access control advantage is good as well as the HABE efficiency is flexible as well as scalable, computational overhead also occur sometimes. Next, HABE scheme is defined by randomized the polynomial time algorithms as follows:

Setup(K) → (params,MK0): Input is taken as sufficiently large security parameter K, and outputs 'params' system parameters then root master key 'MK0'.

CreateDM(params,MKi, PKi+1)→(MKi+1): Generates master keys which is directly using params and its master key.

CreateUser(params,MKi, PKu, PKa)→(SKi,u, SKi,u,a) Initially checks for 'a' 'U' is suitable one, which is administered by itself. If so, it generates a user identity secret key then the user attribute secret key 'U', by using params then its master key; or else, outputs is "NULL".

Encrypt(params;f;A;{PKa|aEA})→(CT): A client takes a record f, a DNF access control strategy An, and open keys of all properties in An, as information sources, and yields a Ciphertext CT.

Decrypt(params, CT, SKi,u, {SKi,u,a|aECCj}→ (f):A user,whose properties fulfill the j-th conjunctive condition CCj, takes params, the ciphertext, the client personality mystery key, and the client trait mystery enters on all qualities in CCj, as contributions, to recoup the plaintext.

2. Attribute-based encryption with privacy preserving key generation scheme (PPKG-ABE) [12] In the key generation period of conventional ABE, KGC consistently knows the attribute data of every client. This has incredibly harmed the privacy of clients. So as to take care of this issue, we separate the two elements of attribute auditing and key extricating. At that point present an Attribute Audit Center (AAC) in ABE framework to authenticate the attributes of clients and to make dazzle token for them. KGC, as a simple technical support institution, is only responsible for generating keys, but it does not know the corresponding attributes of these keys – Setup, UserTemKeyGen, BlindTokenGen, BlindKenGen, KeyExtra, Encrypt, and Decrypt. The specific algorithms are described as follows:

Setup(x)→PP, MK: the KGC run the setup algorithm, then the inputs 'x' security parameter, then it outputs is 'PP' public parameters finaly 'MSK' master secret key.

UserTemKeyGen(PP, k)→TPK_{user},TSK_{user}: the user run user's temporary-key generation algorithm which takes 'PP' then input 'k' is security parameters as well as outputs TPK_{user} user's temporary public key then TSK_{user} user's temporary secret key.

BlindTokenGen(PP, S, TPK_{user})→ T_S: the algorithm for blind token generation which run AAC that takes 'PP', 'S' user's attributes set, then input of TPK_{user} user's temporary public key and outputs a blind token T for attributes set S.

BlindKenGen(PP, MSK, T_S)→ BSK: the KGC is run by blind key generation algorithm which takes 'PP' , 'MSK' master secret key, and input value T_S user's blind token and outputs blind secret key BSK for attributes set S.

KeyExtra(BSK_S, TSK_{user})→ SK_S: the user run the key extract algorithm locally whihc takes BSK_S as blind secret key and input of TSK_{user} user's temporary secret key then outputs of 'SK' final secret key for attributes set S.

Encrypt(PP, M, W)→ CT: the encryptor runs the encryption algorithm which takes 'PP', 'M' message, and input 'W' is access structure and outputs is 'CT' ciphertext.

Decrypt(CT_W, SK_S)→ M: the decryptor runs the decryption algorithm which takes CT_W ciphertext then input is SK_S secret key as well as outputs message 'M', if S ⊨ W.

IV. PERFORMANCE ANALYSIS

Lightweight authentication mechanism performance can be simulated environment as well as measured the performance metrics which is evaluated. Also analyses the performance which ensure the security while authentication mechanism is perform.

Accuracy - Accuracy is the term which refers the measurement result, or calculation can be conforms by the correct value or a standard. The table which depicts the system how accurately works. By categorizing the values, Accuracy can be determined into true positive, false positive, false negative at that point true negative. In the event that the worth is true positive, at that point it goes under the range likewise accurately assessed. False positive worth can be drops out of range however the framework says the worth is inside range. On the off chance that the worth is False negative inside in range however the framework predicts it to not be right. True negative is the worth when the framework demonstrates an inappropriate quality as error.

$$Accuracy = \frac{\sum True\ positive + \sum True\ negative}{Total}$$

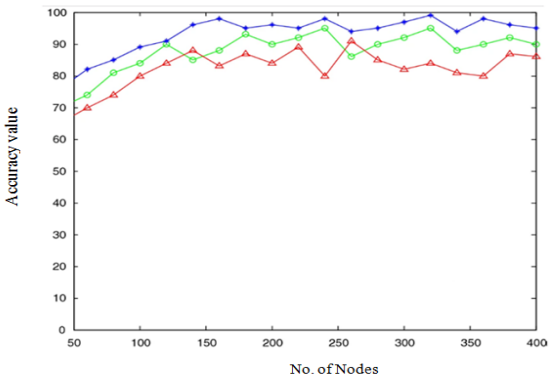

Figure 3: Accuracy calculation with Proposed and existing method

The Above figure 3 shows the comparison graphs of proposed and existing methods. The blue, green and red line shows the Proposed, HABE and PPKG-ABE scheme.

Latency: Latency is defined as the time required for packet to move from one point to another. Latency plays a crucial role in real time applications. In our work, calculated latency in terms of communication latency and data handover latency. Communication latency deals from gateway to end user for authorization and authentication. Data latency deals two gateways for mobility enabled end to end trust scheme. The data handover latency and communication latency are projected on 20 Mb/s internet connection.

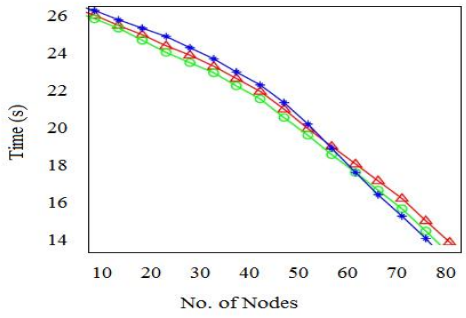

Figure 4: Latency calculation with Proposed and existing method

The Above figure 4 shows the comparison graphs of proposed and existing methods of Latency. The blue, green and red line shows the Proposed, HABE and PPKG-ABE scheme.

Transmission overhead: Transmission overhead is defined as message to be communicate with the number of bits, that do not represent the data message bits.

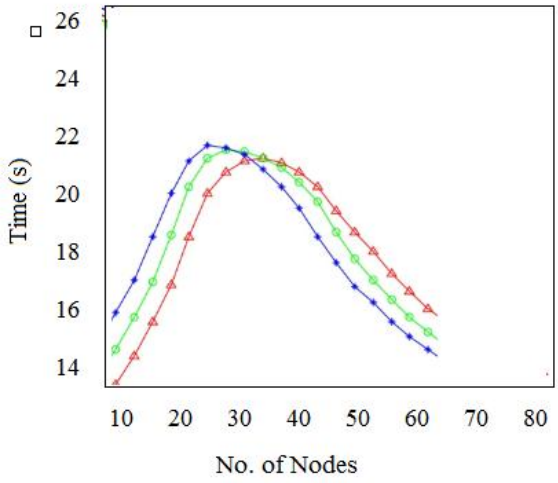

Figure 4: Transmission overhead with Proposed and existing method

The Above figure 4 shows the comparison graphs of proposed and existing methods of Transmission overhead. The blue, green and red line shows the Proposed, HABE and PPKG-ABE scheme.

Table 1: Performance of Proposed and existing methods

Parameters	Proposed Trust based Lightweight Authentication	HABE Scheme	PPKG-ABE scheme
Accuracy	93.41	87.12	68.87
Latency	14.04	25.14	16.87
Transmission overhead	11.78	21.47	22.35

V. CONCLUSION

Recently, the Modern health care environment usage among the IoT technology provide physician convenience as well as patients, while different medical areas are applied namely patient information management, real time monitoring as well as healthcare management. One of the core technology of IoT development in healthcare system is body sensor network (BSN) technology, where patients health conditions are monitors by tiny devices then lightweight wireless sensor node. Still, New technology is developed in healthcare applications without any security considerations that makes the patient privacy vulnerable. The patient's condition can be simultaneously monitored then provide the status to the patients family members. The accuracy can be 93% achieved then the latency and transmission overhead as 14.07 and 11.78 respectively.

REFERENCES

1. P. A. Laplante and N. Laplante, "The Internet of Things in healthcare: potential applications and challenges," IT Professional, vol. 18, pp. 2–4, May 2016.
2. P. Po Yang, O. Amft, Y. Gao, and L. Xu, "Special issue on the Internet of Things (IoT): informatics methods for IoT-enabled health care," Journal of Biomedical Informatics, vol. 63, pp. 404–405, September 2016.
3. K. Lee, "Healthcare IoT security issues: Risks and what to do about them," December 2015; http://searchhealthit.techtarget.com/feature/HealthcareIoT-security-issues-Risks-and-what-to-do-about-them
4. P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," Medical Devices (Auckland), vol. 8, pp. 305–316, Julay 2015
5. Ahmed Abdelaziza, Mohamed Elhoseny, Ahmed S. Salama, A.M. Riad,"A Machine Learning Model for Improving Healthcare services on Cloud Computing Environment", Measurement, Volume 119, April 2018, Pages 117-128, 2018.
6. Nidhi Sharma, Ravindara Bhatt, "Privacy Preservation in WSN for Healthcare Application", Elsevier, Procedia Computer Science, pp. 1243–1252, 2018.
7. Anil Chacko , Thaier Hayajneh," Security and Privacy Issues with IoT in Healthcare", EAI Endorsed Transactions on Pervasive Health and Technology, Vol. 4, Issue. 14, 2018.
8. Wencheng Sun, Zhiping Cai , Yangyang Li, Fang Liu,Shengqun Fang and Guoyan Wang, "Security and Privacy in the Medical Internet of Things: A Review", Hindawi Security and Communication Networks, 2018.
9. Razzaq, M. A., Sheikh, R. A., Baig, A., & Ahmad, A. (2017). Digital image security: Fusion of encryption, steganography and watermarking. International Journal of Advanced Computer Science and Applications (IJACSA), 8(5).
10. Isma Masood, Yongli Wang, Ali Daud, Naif Radi Aljohani, and Hassan Dawood, "Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure," Wireless Communications and Mobile Computing, vol. 2018, Article ID 2143897, 23 pages, 2018.
11. G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.
12. Yujiao Song, Hao Wang , Xiaochao Wei, and Lei Wu, "Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud", Hindawi, Security and Communication Networks, Article ID 3249726, 2019.