A lightweight Security Scheme for IoT based Medical Applications

C Bala Murugan, S Koteeswaran

Abstract – Internet of things (IoT) aims to integrate several smart and heterogeneous devices, technologies, tools etc., through the Internet for remote access and data exchange. The integration of IoT devices and a cloud becomes an attractive solution for elderly people to resolve their health issues instantly without visiting a hospital. However, security of the patient's important health information either during transmission or collecting them are very challenging issue. This aims to introduce an authentication based security scheme for protecting patient's health data in IoT environment using NS2 simulation environment. Our proposed security scheme attain essential requirement and outperforms existing methods.

Keywords – Authentication, Security, Healthcare system, IoT, Cloud.

I. INTRODUCTION

Healthcare is exceptionally imperative for aged people as they can become easy prone to any disease easily. Few common medical barriers include doctors, nurses and beds may affect of offering timely medical treatment and they desire to be active and independent. Rather than visiting a hospital, the demand of offering necessary resources remotely from a medical institution like a hospital is particularly high [1]. The goal of continuously monitoring and follow-up patient's critical signs is really an important key service of a healthcare medical institution. This is typically achieved by attaching smart analytical devices like biosensors into their patient's body and connect them with an external monitoring device [2]. IoT has been recognized as a technology resolution for medical healthcare applications that monitor patient's pathological parameters and has been the focus of many recent researchers [3 – 7]. Several different technologies and components like smart devices, machine learning and processing, wireless communication, etc., are the essential components of IoT. Almost every smart device including biosensors is distributed in an open environment which makes them prone to be assaulted by a third party. In addition, the link between biosensor nodes and users reside in a public channel and a third party or remote attacker can alter messages and eavesdrop in the communication network. Thus, one of the important design issues of the IoT in healthcare system is security; the need of ensuring privacy, confidentiality and authenticity of patient's data [17]. To handle this security issue, it is essential to devise a security scheme which permits the communicating parties to securely share a secret key and also offering confidentiality and authentication services to patient's data over untrusted network. Securing patient's information is very important in an IoT environment. Specifically, guaranteeing the protection of a patient's vital data while in transit like confidentiality, integrity and authentication are mainly key challenges in the modern digital open world. It is typically a basic requirement of offering security to many real time medical healthcare applications which handle sensitive information. Our research paper presented a new authentication based cryptographic scheme for IoT based intelligent healthcare monitoring scheme.

A. Important layer of IoT

Advanced of both Internet technology and minimization of smart computing devices make the IoT becomes essential part of human lives and ensuring security of all its components become vital. With reference to Figure 1, a healthcare IoT system is comprised of three important layers [10].

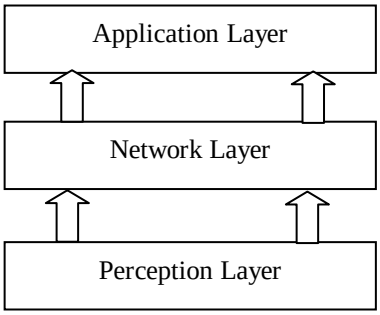

Figure 1 Different Layers of a Healthcare System

- *Perception Layer* – It is responsible for collecting user's/patient's vital biological information from smart devices.
- *Network Layer* – The middle layer comprises wired- and wireless-systems and performs many functions like data processing, information transmission, etc,. Different protocols can be designed to support this layer that needs to be optimized in terms of efficiency and energy consumption. In addition, security and privacy requirements also very important.

Revised Manuscript Received on April 07, 2019.

C Bala Murugan, Research Scholar, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India. And Assistant Professor, Department of Computer Science and Engineering, V V College of Engineering, Tirunelveli – 627657, TamilNadu, India.

S Koteeswaran, Associate Professor, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India.

- *Application Layer* – This layer called user view interface integrates different data resources and provide them necessary information to the end-user on demand basis.

Suitable protection strategy could be designed based on the requirements and purpose. There are many security principles like CIA principles (Confidentiality, Integrity and Availability), authentication, possession, non-repudiation should be considered for security IoT components. However, authentication concern becomes more important in the IoT environment; because it will directly affect CIA principles. An adversary can be skilled enough as a legitimate user and perform any task like reading user's sensitive data, modifying data and confine availability of data which would compromise the CIA principles. Thus, the security and privacy of medical application which handles patient's sensitive biological healthcare data remains a major challenge.

B. Authentication within healthcare IoT

The authentication system as shown in Figure 2 considers two different circumstances i.e. home and medical institution like a hospital. Both arrangements include different smart devices like actuators and biosensors which would facilitate the daily activities of aged people. Each device of an IoT system is connected to the Internet through central device using wired- or wireless-communication. The users of the scenarios can communicate and handle the information instantly at any time through appropriate IoT supporting device.

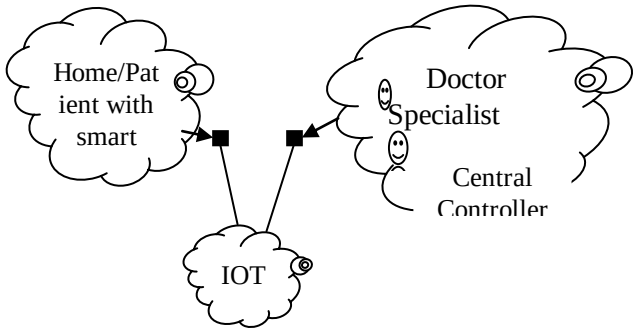

Figure 2 Authentication service in IoT Healthcare system

C. Threat Prototype

We employee extensively accepted threat model namely, Doya [8] in which the data exchange between two communicating parties are typically carry out over a public open channel. A remote attacker can launch an eavesdropping attack like read, alter or delete any content of the data packets actually being sent. In addition, the attacker still able to compromise any smart device in IoT environment and can steal some vital data cached in it through a power inquiry attack [9].The foremost part of our work incorporates the following.

i. We present an enhanced secure cryptographic based authentication scheme to resolve the aforementioned security issues.

ii. To prove the security strength of our authentication scheme, we consider Burrows-Abadi-Neeham (BAN) logic to ensure the trustworthiness of the message being exchanged against eavesdropping attack.

iii. We use NS2 too for formal measuring parameters that affect the performance of the underlying network.

iv. Finally, we argue that the proposed scheme outperforms the existing designs in terms of cost for different operations.

The remaining sections of the paper are prepared as follows.Section 2 describes security challenges, issues and requirements of IoT in healthcare system. Section 3 briefly discusses few existing works done in the past and Section 4 presents our proposed security scheme. Section 5 talks about the performance analysis and comparative of our scheme compare to existing solutions in IoT environment respectively. Finally, Section 6 points out our final conclusions.

II. SECURITY REQUIREMENTS AND CHALLENGES OF IOT HEALTHCARE APPLICATIONS

IoT healthcare applications might offer different services to elder people like remote-health monitoring with prescriptions, handling emergency case, detecting nearest healthcare institutions such as ambulance service, doctors, vital medicines, etc. Typically, healthcare of people, specifically aged people is very important and has a vital force on their daily lives [10]. There exist many solutions to design an IoT technology offering various healthcare services [11]. Basanta et al. [12] implemented a framework namely, help-to-you remotely monitor vital parameters of aged people. Yang et al. [13] integrates traditional mecial healthcare technology with smart medical healthcare services. They used medical boxes like iMedPack, iMedBox, etc., to offer different services. Fan et al. [3] implemented a rehabilitation scheme for IoT using optimal resources. Their proposed design used semantic data to effectively discover important healthcare resources of a medical institution.

In order to keep patien's healthcare record and their residential information confidential is very important. Ding et al. [14] focused on working security issues of medical IoT system. The authors focused on ensuring security of patient's electronic healthcare records, residential location and identification, medical queries. Gong et al. [15] proposed an effective algorithm for implementing a smart healthcare medical system. Their algorithm more importantly utilized improved DES private encryption algorithm and private homo-morphism to offer and ensure the confidentiality of a patient's data while in transit and also in server.

We list some design requirements of IoT medical healthcare applications to counteract eavesdropping attacks.

- *Trust* – IoT applications are distributed and dynamic in nature. Ensuring the trustworthiness among interacting devices is most important. Restriction of usage of power is also a vital issue of a trust management being developed.
- *Privacy* – Ensuring privacy of patient's vital medical parameters is really a mandatory service to be offered. The privacy concern aims areas like data monitoring, collection, sharing and security.

- *Reliability* – It is an essential requirement, which guarantee data and service availability.
- *Mutual Authentication* – It aims to ensure the identities of entities of all communicating parties during communication. This can be achieved by permitting each party to authenticate each other.
- *Key Usability* – The use of a session key is very essential in nay authentication scheme. It is mainly utilized to strongly secure communications against third party attacks.

III. RELATED WORKS

Both security service and privacy service to patient's healthcare are not indispensable ideas. Security to a patient data can be achieved using cryptographic algorithms which offer different technological ideas for securing the data being exchanged and the communication channel [16] using some kind of authentication scheme. A simple key management security scheme for protecting end-to-end communication has been presented in [17]. This solution dealt heterogeneous types of devices with various properties. In addition, the proposed scheme relies on utilizing session keys against man-in-middle attack and also consumes minimal resources.

Implementing privacy issues to IoT based applications become vital design issue of a smart medical healthcare system. Hu et al. [18] designed a cloud technology to remotely monitor a patiten's personal and biological parameters. The proposed solution combines many technological features like signature, digital certificates, digital envelope, time-stamps and public key cryptographic algorithms to offer stronger and flexible medical services. The authors claimed that their solution utilized only minimal medical resources. However, the computation coasts may increases.Li et al' [19] implemented a robust authentication security scheme based on key agreement scheme for WBAN-medical healthcare system. It relies on chaotic maps and cloud technology. In this approach, each participant must register before transmitting encrypted data. This can be achieved using Diffie-Hellman key exchange algorithm. The authors utilized cloud technology for efficiently handling, processing and storing huge amount of patient's data dynamically. Similar approach but addressed the relationship between cryptographic- and non-cryptographic technique has been proposed in [20]. This security scheme comprised of three important parts: patient, medical institution and a cloud. The proposed signature based authentication and authorization protocol relies on discrete log based hashing technique. Lounis et al. [21] presented a cloud based security policies based on access control for medical healthcare system. It mainly used the idea of attribute based ciphertext encryption policy scheme. The authors by simulation experiments proved that the developed scheme is scalable and efficient. As patient's vital data can be stored in third parties without consent of the user could compromise a cloud, its consistency and integrity. Govaert et al. [22] review the relationship importance of operating and auditing costs of patient's data stored in a cloud. Similarly, searching and retrieving exact data from a cloud also affects the performance of the underlying environement. Bezawada et al. [23] designed a private key based encryption scheme to search and extract exact input string in a cloud environement. Ut relies on a pattern based secure binary search tree and relevance-ranking algorithm to effectively process a user's query. Lin et al. [24] developed a clustering based k-anonymity approach that supports privacy for smart wearable devices. The proposed set of rules produces a table of data that would strengthen the identities of a user against eavesdropping attacks.Recent technology advancement provides flexibility of implementing various medical resources for aged people/users seeking instant medical advice and service. Though many existing solutions offer different IoT based medical services to users but implementing strong security measures still immature.

IV. PROPOSED SECURITY SCHEME

This section presents a novel security model based on key generation and authentication schemes for medical based IoT applications. As shown in Figure 2, the communication can happen between end-users (patient, doctor, nurse, etc.) and smart healthcare devices using a Central Controller (CC) to offer secure communication. In our proposed security model, each participant should register with the CC that offers secure communication between different users. A user can also gets a session key with time-stamp; they can be generated for ensuring confidentiality of patients vital data and also avoid replay attacks. Aged people can use any smart device like a smart phone to communicate with any IoT based medical sensor which is responsible for collecting patients biological information. Various notations that are used in the proposed scheme are listed in Table 1.

Table 1 Notations used

A	Aged people
I	Medical Institution
KAC	Key Manipulation and Authentication Centre
HSS	Healthcare Smart Sensor
SMP	Smart Mobile Phone
S	Session key
RP	Registration Phase
Pwd	Password
ID_A	Identifier of a patient
ID_I	Identifier of a medical institution
ID_M	Mobile Device Identifier
PU	Public key
PR	Private key
r	Random Number
t	Time Stamp
C	Cloud
Cert	Digital certificate
MD	Medical Data

Sic	Signature
IM	In-case-of-emergency

4.1. Registration Phase

Each participant, specifically the aged patient and medical institution may register on the KAC to prove their legitimaticity. The KAC will generate a pair of keys (private, public) to each participant/user using RSA cryptographic mechanism. The user will receive the public key together with a session key to secure a patient's vital medical data. The important steps of the RP are as follows.

i. An aged patient and medical institution choose their identities like ID_A, ID_I, pwd and post then to the KAC using a secure channel. The patient also post their additional information like personal- and emergency-contacts, ID_M to KAC.

ii. The KAC generates a pair of key (PR, PU) and key S for each participant and medical institution separately.

Key PR of A, $PR_A = h_0(ID_A, r)$

Key PR of I, $PR_I = h_0(ID_I, r)$

and

Key of A, $S_A = h_1(PR_A, r, t_{KAC})$

Key of I, $S_I = h_1(PR_I, r, t_{KAC})$

Afterwards, the KAC performs the following operations

$$KAC \rightarrow (PU_A, PR_A, S_A)$$

$$KAC \rightarrow (PU_I, PR_I, S_I)$$

$$KAC \rightarrow (cert_A)$$

$$KAC \rightarrow (cert_I)$$

In order to support scalability and safety, we use a cloud environment to keep patient's vital information. Thus, the KAC also performs the following operations.

$$KAC \rightarrow (PU_C, PR_C, S_C)$$

iii. Each participant A, KAC, and I keeps their PU, PR and S safely. And, A and I use their respective certificates to perform authentication.

4.2 Information Upload Phase

This phase consists of Data Upload through SMP, Upload Case-report after physical visit and In-case-of-emergency which are explained below:

4.2.1 Data Upload through SMP

We consider the IoT based HSS is inlaid into a patient's body. *A* can use a SMP to transmit data collected from HSSs to the cloud.

i. An IoT based HSS collects a patient vital medical data, MD_x and transmits it to the mobile phone over a secure transmission channel.

$$MD_x = \{ID_A, Data_{x1}, Data_{x2}, ...Data_{xn}, S_x)$$

ii. After SMP received the data from step (i), it uses the key S to encrypt MD and includes timestamp t_{SMP}. Next, the mobile phone uses the key PU_c to encrypt the following.

$$MD_{SMP1} = \{ID_{SMP1}, MD_x, t_{SMP1})$$

$$C_1 = S_E(MD_{SMP1})$$

$$C_2 = E_{PU_C}(S)$$

Then, the mobile phone transmits ID_A, $cert_A$, C_1, C_2 and t_{SMP1} to the cloud.

iii. Now, the cloud checks whether t_{SMP1} is recent or not.

$$t_{C_1} - t_{SMP1} \leq \Delta t$$

If the above condition is true, the cloud checks whether the ID_A stored in its datastore reflects the identity of the respective user (A). And then, the cloud uses PU_{KAC} to validate the certificate of A. Finally, the cloud uses PR_C and S_C to encrypt C_1 and C_2.

4.2.2 Upload Case-report after physical visit

The aged patient may visit a hospital for a normal check-up and his/her case-report will be stored into the cloud after successfully validating the authentication phase of I and C.

i. The hospital uses the key S_C to encrypt case-report of a patient with timestamp t_{I1}. Then, I uses PU_C to encrypt S_C and manipulates a signature Sic_1 as follows.

$$MD_{h_1} = (ID_I, ID_A, Data_{h_1}, Data_{h_2}, ...Data_{h_n}, t_{h_1})$$

$$C_3 = PR_{S_C}(MD_{h1})$$

$$C_4 = E_{PU_C}(S_C)$$

$$Sic_1 = S_{PR_I}(h1(MD_{h1}))$$

Next, I sends ID_I, ID_A, Sic_1, $cert_I$, C_3, C_4 and t_{I1} to the cloud.

ii. Now, the cloud validates the signature of I using ID_I and checks whether t_{I1} is recent or not.

$$t_{C_3} - t_{I1} \leq \Delta t$$

If the above condition is valid, the cloud applies the KAC's PU_{KAC} to validate $cert_I$. Next, the cloud computes PU_{S_C} using ID_I uses PR_C and S_C to encrypt C_3 and C_4.

$$V_{PU_I}(Sic_1) \stackrel{?}{=} h_1(MD_{h_1})$$

$$S_C = D_{PR_C}(C_3), (ID_I, ID_A, Data_{h_1}, Data_{h_2}, ...Data_{h_n}, t_{h_n})$$

and $S_C = PU_{S_C}$

Finally, the cloud keeps Sic_{h_1} and MD_{h_1} in its local database for future reference.

4.2.3 In-case-of-emergency

Whenever the cloud receives patient medical information from the mobile phone, it immediately compares such data with the data stored in its database. If the comparison indicates an emergency then the cloud raises an emergency alter to the hospital and send off an ambulance to offer immediate-care service, if necessary.

i. Conversation between HSS and SMP

$$HSS \rightarrow SMP : MD_{HSS_2}(ID_A, Data_{HSS_1}, Data_{HSS_2}, ...Data_{HSSn}, t_{HSS_2})$$

$$SMP : MD_{SMP_2}(ID(SMP), MD_{HSS_2}, t_{SMP_2})$$

$$C_5 = PR_{S_C}(MD_{SMP2})$$

$$C_6 = E_{PU_C}(S_C)$$

$$Sic_1 = S_{PR_C}(ID(SMP))$$

ii. Conversation between SMP and C

$$SMP \rightarrow C : (ID_A, Sic_2, cert_A, C_5, C_6, t_{SMP_2})$$

$$C : if\ (t_{C_5} - t_{SMP_2}) \leq \Delta t$$

$$S_C = D_{PR_C}(C_6)$$

$$(ID(SMP), MD_{HSS_2}, t_{SMP_2}) = PU_{S_C}(C_5)$$

Verification of $Cert_A$

$$V_{PU_P}(Sic_2) \stackrel{?}{=} ID(SMP)$$

$$MD_{C_3} = (ID_C, ID_A, MD_{IM}, t_{C_3})$$

iii. Conversation between C and I

$$C \rightarrow I : (ID_C, ID_A, C_7, cert_A, cert_C, t_{C_3})$$

$$I : if\ (t_{C7} - t_{C_3}) \leq \Delta t$$

Verification of $Cert_A$

$$MD_{C_3} = D_{PR_I}(C_7)$$

$$MD_{I_2} = (ID_A, ID_I, cert_A, cert_I, MD_{IM}, t_{I_2})$$

$$C_8 = E_{PU_A}(MD_{I_2})$$

iv. Conversation between I and A

$$I \rightarrow A : (ID_I, ID_A, cert_I, cert_A, C_8, t_{I_2})$$

$$A : if\ (t_{C8} - t_{I_2}) \leq \Delta t$$

Verification of $Cert_I$

$$MD_{I_2} = D_{PR_I}(C_8)$$

V. SECURITY ANALYSIS

This section discusses security analysis of our proposed scheme against various attacks. Privacy – Internet is open network in nature. Therefore, security is very important during data transmission of patient's vital medical information. In our scheme, privacy is offered through encrypting patient's data.Confidentiality – The proposed scheme uses public key cryptography to assure the confidentiality of patients personal data. In addition, confidentiality is assured in different steps during transmission of patients personal data. For example, the mobile phone uses key S_C and the cloud's PU_C to encrypt patient's data. Therefore, the proposed security scheme offers confidentiality service. Integrity – During data exchange operation, the mobile phone's identity like IMEI number has been authenticated.

$$V_{PU_A}(Sic_2) \stackrel{?}{=} ID(SMP)$$

Therefore, our proposed security scheme is strong enough against tampering the mobile phone's identifier.

A.Replay attack – Our proposed method uses the utilization of time-stamp to combat against replay attacks. During data transmission, the recipient verifies whether data received is most recent. Thus, replay attacks can be avoided.

B. Man-in-middle attack – Our proposed security scheme resists from man-in-middle attack through checking whether the time-stamped data is most recent or not. Moreover, certification scheme is applied between A, I and C to prove their identities. Thus, a third party cannot get involve any illicit operation during data transmission without key, S and the private key, PR.

5.1 Comparison of Security Analysis

In order to evaluate the security strength of our proposed scheme, we compared our scheme with the schemes developed by Kalra et al. [25] Lounis et al. [26] and Hu et al. [18] based on various security issues as shown in Table 2.

Table 2 Security comparison of our method using different security issues

Security Issue	Kalra et al. [25]	Lounis et al. [26]	Hu et al. [18]	Propose d
Privacy	No	No	Yes	Yes
Confidentia lity	Yes	Yes	Yes	Yes
Integrity	No	Yes	Yes	Yes
Replay attack	Yes	No	Yes	Yes
Man-in-mid dle	Yes	Yes	Yes	Yes
Authenticati on	Yes	No	Yes	Yes

In Table 2, both solutions proposed by Kalra et al and Lounis et al have suffered from privacy issues. In addition, kalra's approach failed to offer integrity service and Lounis method suffers from replay attack and authentication issue. Though our proposed security scheme offers same kind of services as the solution presented by Hu et al., our approach incurred minimal cost in terms of computation and communication.

5.2 Discussions

In order to offer strong secured medical services to aged people, there are many operations have been applied among different entities during communication. The costs incurred by them have measured and tabulated as shown in Table 3.

Table 3 Cost computation of our approach

Case Type	Cost
Uploading case-report to C	$2t_{id}+t'_s+t'_{sic}+t_t+t_{cert}$
Uploading Patient's medical data to C	$T_{id}+t'_s+t_t+t_{cert}$
Handling in-case-of-emergency	$5t_{id}+t'_s+t'_{sic}+3t_t+5t_{cert}$
Ordinary case	$T_{id}+t_t+t_{cert}$
Total	$9t_{id}+3t'_s+2t'_{sic}+6t_t+8t_{cert}$

From Table 3, the highest cost incurred during handling in-case-of-emergency operation with cost=$5t_{id}+t'_s+t'_{sic}+3t_t+5t_{cert}$ = 5*80+1*256+1*1024+3*16+5+8192 = 42,688 bits and the transmission time for handling such operation is 0.2134 ms under the network with bandwidth of 20 mbps.

VI. CONCLUSIONS

Continuously monitoring health condition of aged people and offering either normal or immediate solution is very important. As a solution, we proposed a sensor based medical healthcare security scheme for IoT applications. We exercise SHA-256 hash algorithm, digital certificate scheme and RSA cryptographic mechanism to offer stronger security service for IoT based medical applications. Our proposed light weight security scheme offers secured medical services like CIA and also flexible. It avoids many third party attacks. As our future work, we focus to design stronger certificates based on patient's biometric data which offers stronger authentication service for medical environment.

REFERENCES

1. E.Perrier, "Positive Distruption: Healthcare, Aging and Participation in the Age of Technology", Sydney, NSW:Mckell Institute.
2. H. BaldusK. KlabundeG. Müsch, "Reliable Set-Up of Medical Body-Sensor Networks", Proc. of the European Workshop on Wireless Sensor Networks, pp. 353-363, 2014.
3. Yuan Jie Fan, Yue Hong Yin, Li Da Xu, Yan Zeng, Fan Wu, "IoT-Based Smart Rehabilitation System", IEEE Transactions on Industrial Informatics, Vol.10 , Issue 2, pp. 1568 - 1577, May 2014.
4. Cristian F. Pasluosta, Heiko Gassner, Juergen Winkler, Jochen Klucken, Bjoern M. Eskofier,"An Emerging Era in the Management of Parkinson's Disease: Wearable Technologies and the Internet of Things", IEEE Journal of Biomedical and Health Informatics, Vol.19, Issue 6, pp. 1873-1881, Nov. 2015.
5. Ni Zhu, Tom Diethe, Massimo Camplani, Lili Tao, Alison Burrows, Niall Twomey, Dritan Kaleshi, Majid, "Bridging eHealth and the Internet of Things: the SPHERE Project", IEEE Intelligent Systems, Vol. 30, Issue 4, pp. 39 - 46, July-Aug. 2015.
6. Shih-Hao Chang, Rui-Dong Chiang, Shih-Jung Wu, Wei-Ting Chang, "A Context-Aware, Interactive M-Health System for Diabetics", IT Professional, Vol.18, Issue.3, pp. 14 - 22, May-June 2016.
7. Prosanta Gope, Tzonelih Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network", IEEE Sensors Journal, Vol. 16, Issue.5, pp. 1368 - 1376, March1, 2016.
8. D. Dolev, A. C. Yao, "On the security of public key protocols". Proc. of the 22nd Annual Symposium on Foundations of Computer Science (SFCS '81), pp.350-357, October 28 - 30, 1981.
9. T.S. Messerges, E.A. Dabbish,R.H. Sloan, "Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computers, Vol.51, Issue 5, pp.541 - 552, May 2002.
10. Mauricio García, "The Impact of IoT on Economic Growth: A Multifactor Productivity Approach", Proc. of 2015 International Conference on Computational Science and Computational Intelligence (CSCI), 7-9 Dec. 2015.
11. Muneeb ahmed sahi,haider abbas, kashif saleem,xiaodong yang, abdelouahid derhab,mehmet a. orgun, waseem iqbal,imran rashid, asif yaseen "Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions". IEEE Access, Vol. 6, pp. 464-478, 2018.
12. Haobijam Basanta, Yo-Ping Huang,Tsu-Tian Lee,"Intuitive IoT-based H2U healthcare system for elderly people", IEEE 13th International Conference on Networking, Sensing, and Control (ICNSC), April 2016.
13. Geng Yang, Li Xie, Matti Mäntysalo, Xiaolin Zhou, Zhibo Pang, Li Da Xu, Sharon Kao-Walter, Qiang Chen, Li-Rong Zheng, "A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box", IEEE Transactions on Industrial Informatics, Vol.10, Issue.4, pp. 2180 - 2191, Nov. 2014.
14. Ding Ding, Mauro Conti,Agusti Solanas,"A smart health application and its related privacy issues". Proc. of 2016 Smart City Security and Privacy Workshop (SCSP-W), 11-11 April 2016.
15. Tianhe Gong, Haiping Huang, Pengfei Li, Kai Zhang, Hao Jiang,"A Medical Healthcare System for Privacy Protection Based on IoT", 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), 12-14 Dec. 2015.
16. Yunlei Zhao, "Identity-Concealed Authenticated Encryption and Key Exchange", ACM CCS 2016, October 2016.
17. Mohammed Riyadh Abdmeziem, Djamel Tandjaoui, "A Cooperative End to End Key Management Scheme for E-health Applications in the Context of Internet of Things", Proc. of International Conference on Ad-Hoc Networks and Wireless, pp. 35-46, 2015.
18. Jin-Xin Hu,Chin-Ling Chen,Chun-Long Fan, and Kun-hao Wang, "A n Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing". Journal of Sensors, Vol. 2017, pp. 1-11, 2017.
19. Chun-Ta LiCheng-Chi Lee, Chi-Yao Weng, "A Secure Cloud-Assisted Wireless Body Area Network in Mobile Emergency Medical Care System". Journal of Medical Systems, May 2016.
20. Santosh Chandrasekhar, Ahmed Ibrahim, Mukesh Singhal,"A novel access control protocol using proxy signatures for cloud-based health information exchange", Computers & Security, Vol. 67, pp.73-88, June 2017.
21. Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah ,Yacine Challal,"Secure Medical Architecture on the Cloud Using Wireless Sensor Networks for Emergency Management", Proc. of Eighth International Conference on Broadband and Wireless Computing, Communication and Applications, Oct. 2013.
22. Johannes Arthuur Govaert, Anne Charlotte Madeline van Bommel, Wouter Antonie van Dijk, Nicoline Johanneke van Leersum, Robertus Alexandre Eduard Mattheus Tollenaar, and Michael Wilhemus Jacobus Maria Wouters, "Reducing Healthcare Costs Facilitated by Surgical Auditing: A Systematic Review", World J Surg. Vol. 39(7), pp. 1672–1680, 2015.
23. Bruhadeshwar Bezawada, Alex X. Liu, Bargav Jayaraman, Ann L. Wang, Rui Li, "Privacy Preserving String Matching for Cloud Computing", Proc. of IEEE 35th International Conference on Distributed Computing Systems, 2015.
24. Fang Liu and Tong Li, "A Clustering k-Anonymity Privacy-Preserving Method for Wearable IoT Devices", Security and Communication Networks, Vol.2018, pp .1-8, 2018.
25. Sheetal Kalra, Sandeep K.Soodb,"Secure authentication scheme for IoT and cloud servers".Pervasive and Mobile Computing, Vol.24, pp.210-223, December 2015.
26. Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah, Yacine Challal,"Healing on the cloud: Secure cloud architecture for medical wireless sensor networks", Future Generation Computer Systems, Vol. 55, pp. 266-277, February 2016.

AUTHORS PROFILE

Mr C. Balamurugan, currently pursuing his Ph.D in the Department of Computer Science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai-62, Tamilnadu, India. He is working as an Assistant Professor in the Department of Computer Science and Engineering at V V College of Engineering. Prior to this he was associated with Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi , Chennai. He obtained his B.E (CSE) from Dr. Sivanthi Aditanar College of Engineering College (Anna University, Chennai) and M.E (CSE) from Vel Tech Multitech Engineering college (Anna University, Chennai). He has been in the teaching profession for the past 9 years and has handled both UG and PG programmes. His areas of research are Wireless Sensor Networks and Internet of Things (IoT). He has published 6 research articles in International Journals and 3 papers presented in National Conferences. He has attended various Training Programmes, Workshops and FDPs related to his area of interest.

Dr. Koteeswaran Seerangan, currently working as an Associate Professor in the Department of Computer Science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai-62, Tamilnadu, India. He has authored and co-authored several papers in various reputed journals and conference proceedings. He is a reviewer for more than a dozens of journals. His research interests include Theory of Computation, Software Engineering, Data Mining, Big Data and Cloud Computing. He is a Member of ACM, Member of IET, Senior Member of IEEE and Life Member of ISTE.