Secured Architecture for Internet of Things (IoT) Based Smart Healthcare

A. Vimal Jerald
Department of Computer Science
St. Joseph's College (Autonomous)
(Bharathidasan University)
Tiruchirappalli, Tamilnadu, India
vimaljerald@gmail.com

Dr. S. Albert Rabara
Department of Computer Science
St. Joseph's College (Autonomous)
(Bharathidasan University)
Tiruchirappalli, Tamilnadu, India
a_rabara@yahoo.com

***Abstract*—Internet of Things (IoT) plays a vital role in making human lives smarter. Variety of IoT applications and services are deployed day by day with the tremendous efforts of Information Technology today. As the IoT applications and services bring forth numerous benefits, there also potential threats such as security while implementing these IoT based smart applications. Health Care is a major domain in which IoT can be used to deploy smart health care. This article puts forward a secured architecture for IoT based smart health care. The architecture proposed enables a secured transaction of health care data from the patients to IoT Health Seva Kendra that processes or aggregates the data to facilitate the healthcare practitioners with the necessary information.**

Keywords— Internet of Things (IoT), IoT based Health Care, IoT Information Kendra (IoT IK), Elliptic Curve Cryptography.

I. INTRODUCTION

IoT consists of things such as objects and sensors connected using communication capabilities infer information to compute, analyze and aggregate for decision making. IoT devices and objects play a major role in business and different social relevant processes to communicate and interact between them and with the environment by using data exchange [1]. IoT has become very popular in digital world today because of some potential applications such as smart farming, smart health care services, smart traffic control, smartcity projects etc.,[2]. Various research groups of Melbourne, Australia have identified Health care, emergency services, transport, crowd monitoring, defense, whether monitoring and water quality management as fewer applications of IoT whihc are potential [3]. There will be approximately 40 smart cities across the globe by 2025. The evolution of smart cities will be of Smart Economy, Smart Healthcare, Smart Citizen, Smart Mobility, Smart Buildings, Smart Energy, Smart Information and Communication Technology, Smart Planning, and Smart Governance. [4].

Smart Healthcare is a major application domain of IoT. In the recent years, this domain has attracted more attention from academicians and researchers to address the potential of the IoT in the health care field. Taking into consideration of numerous practical challenges, there are variety of services, applications and prototypes in the domain. IoT based Smart Healthcare research includes network architectures and their platforms, interoperability, hetrogenity, security, new services and applications. Guidelines and policies are framed for devloping the IoT technology in the field of medicine. Inspite of all these efforts, still IoT remains in its infancy in the healthcare domain. Hence it is essential to have a thorough understanding of contemporary research on the IoT based healthcare which will certainly benefit different stakeholders interested in the future research. [5]. This article deals with a secured architecture for Internet of Things (IoT) based Smart Health care system.

II. REVIEW OF LITERATURE

Ngo Manh et. al., have proposed IoT based remote health monitoring system. The proposed system has five layers such as sensing layer, home gateway layer, network infrastructure layer, cloud computing layer and application layer. The sensing layer with sensors and actuators which is responsible for inferring data for aggregation Gateway layer is responsible for filtering or pre-processing and transmits the data for next level. Encryption is also carried out as the health relevant data need to be protected as it is more sensitive. In the cloud layer, sensor data is transformed into meaningful data and action using appropriate algorithm and with intention of software. Data storage is done with efficiency and elasticity is in cloud storage service. The application layer interacts with the user through application and web interfaces. The prototype implementation is carried out using CoAP and HTTP separately. The implementation result shows that the implementation using CoAP considerably reduced the requirements of bandwidth and the volume of generation data for the healthcare data, the no of packets sent reduced significantly. It is conducted that IReHMO is capable of deploying healthcare IoT services using IoT devices. For encryption of data 128 bits AES algorithm is used in the proposed work which is not efficient as of RSA, DSA and ECDSA. Hence, it is essential to improve the encryption tech methodologies using ECDSA which is comparatively efficient [6].

Danilo et. al., have proposed IoT architecture for health information sharing system. The system uses various health managers and gateways by maintaining interoperability using the standards. The health manages such as mobile devices and cloud application are distributed in different locations by making use of a single health service for variety of personal health devices. The health sensors attached in the users body and the measured parameters are identified by health managers. The managers are further connected to the health solution. The Personal Health Devices (PHDs) are technologies like Bluetooth to share information to reach the cloud using smart phones. Internet Health manager is another component of the proposed architecture which makes feasible to Internet ready PHDs to transmit data directly to the internet using internet gateways. Different standards and protocols are used for actualizing the system which are CoAP and HTTP protocols. The proposal system is implemented with its prototype and the report said that the system will be very much opting for the health domain using IoT. It is important to extend this work as secured and scalable for the real time implementation [7].

Daeil kawon et. al., have explored the concept of prognostics Health Management system for industrial application using IoT. The four dimensions of PHM discussed in the article are sensing, prognosis Diagnosis and Management. RFID tags and embedded sensors collect the data and the collected data is transmitted via network communication for the processing. The cloud is used for computation by using application and software platforms. People are able to access the data stored in cloud. The security is given emphasis for the entire architecture by different levels of authentication. The presented system is applicable for different sectors of industries like manufacturing heavy industry infrastructure, transport and logistics, automobiles, Robotics. It is cited that IoT based PHM scheme oriented data are sensed by wireless sensors which are sent to a base system or computer for analysis. RFID, Bluetooth, Wifi, WiMax are few transmission techniques used. There is a possibility of threat to data integrity by malicious software and hence, the trust worthiness of IoT based PHM system is questioned. So, the security issue such as data integrity has to be addressed. It is concluded that IoT based PHM will have its impact in prediction, risk mitigation and reliability assessment. The security of data is the biggest concern which needs to be addressed [8].

S.M. Rlazul et. al., have made a survey on IoT based healthcare technologies and have reviewed different architecture, application for IoT based health care solutions. It is reported that IoT network for health care is of the significant element of IoT healthcare. It facilitates the transmission and reception of health care tailored communication. The IoT health care network is composed of three major components such as topology, architecture and platform. The article reported that patient's health profile and health data is inferred with the help portable medical devices and sensor attached to the body. The data inferred are then analyzed and stored for data aggregation. Based data aggregation and analytics, the care givers can monitor the patients based on the geographical location another scenario namely IoT Net topology is presented in the article. IoT devices, things and sensors are connected wirelessly to health care gateway which connects the patient's environment to IoT health cloud and heterogeneous network (HetNet) for analysis and diagnosis of health issues. The gateway itself is used for analysis, storage and display of collected data. The various healthcare services and healthcare applications are discussed and some of them are glucose level sensing, electro cardiogram monitoring, BP monitoring, and body temperature monitoring, oxygen saturation monitoring. Health care devices and application deal with personal health related data. There is possibility of a hackers targeting IoT healthcare. It is essential to ensure the security requirements like privacy, confidentiality, integrity, authentication, availability, authorization, fault intolerance and self-healing. To overcome these security issues, security models need to be developed using its dynamic properties [5].

Luliana et. al., have proposed a general architecture for healthcare system for monitoring patients in the ICU using the concept of IoT. The article reported that the variety of sensors and or sensing devices are connected with the patient's body which is connected with ICT monitors via wires. The sensor devices transmit electronic signals to ICU monitor. The monitor displays specific signals and may alert the medical staff by giving alarm to take care of the patient. There may be problem of removal of sensing devices wire, when patient move and so the patient will be at risk. To mitigate this issue ICU based monitor used to monitor patients record and Kinect sensors monitor the movement of the patient. There is a concept called Natural User Interface (NUI). Skelton tracking system is used for managing the properties of the detached Skelton. Accelerometer is used to measure vibrations in the patient's body. The sensed data from sensors are sent to the internet for the analysis. The information is sent to the servers where users are connected. The health records stored is a server may be accessed by the doctor using interface which is user friendly. Web band health monitoring application will analyze and process the data from every device of ICU and informs the doctors about the change of parameters of the patient's body. The authors concluded the proposed system is opt for the health care service particularly for the people who need permanent monitoring or support. The system needs to be tested and as the patients personal information is involved, it is important to ensure privacy and the security concerns. The systems could be extended for more health related application using more new types of health sensors [9].

The article by saikiran et. al., has reported the ECG data acquisition and transmission architecture based on IoT. The architecture consists of ECG data acquisition system which collects ECG by electrodes that are attached to the human body for the monitoring the data. ADC is used to convert Analog ECG data to Digital data which is stored for sampling with the records of different patients. The ECG signals obtained are analyzed based on different parameters such as P,Q,R,S,T. P in ECG represents depolarization. T gives the actual and ventricular depolarization using the signal processing algorithms patients' health is monitored remotely by extracting data. Another main component of the architecture is proposed rule engine. There are two types of rule engine namely Static rule engine and Adaptive rule engine. Patient's health condition is decided whether normal or abnormal based on the data extracted. Some cases using static rule engine with single hand threshold will be efficient in case of patient suffering major block. In such cases, Adaptive rule engine is used, in which the data exceeds hand threshold which leads to transmission of data continuously. The article concluded that the proposed system will be more useful in IoT based healthcare systems with solutions for envisioned security issues [10].

Udit et. al., have come out with IoT based Healthcare monitoring system using Real time signal quality aware ECG telemetry. The IoT enabled ECG monitoring framework uses Arduino, Android phone, ECG sensors, and Bluetooth and cloud server. The Signal Quality Aware (SQA) IoT framework is composed of three modules namely ECG signal sensing module, automated signal quality assessment module and SQA ECG analysis and transmission module. The automated ECG signal quality assessment method and the SQA IoT framework is evaluated under different activity conditions. It is also performed to grade the ECG signal acquired with decision score. The proposed SQA IoT framework is tested with various ECG recording under nesting ambulatory and physical activities under standard metrics. It is concluded that SQA IoT enabled Telemetry system is very much applicable for the cardiac health monitoring applications. It will be a fool proof system when the anticipating security issues are appropriately addressed [11].

IoT based smart healthcare is of multifaceted in nature. Integrated networking, information processing, sensing and actuation capabilities allow physical devices to operate in changing environments will certainly have very many challenges and some of the issues and challenges[12]. Confidentially, integrity, availability and authentication are the security measures which must be lightweight and heterogeneous in nature. It is proposed to define policies and standards to ensure that the data will be managed, protected and transmitted in an efficient way. There is also a need for lightweight key management system for enabling trust between different things used in IoT.[13]. Mikael et.al., have explored the security requirement; in critical societal services namely energy, water and health management systems. The authors have presented the security difficulties in IoT deployment. It is said that the biggest challenge from the device side is that aIoT of M_2M/IoT device do not have enough capability to do the encryption on the device. It is proposed to enable lightweight intrusion detection by implementing memory efficient representations and CPU efficient algorithm in real time [14].

Hence, a unique secured architecture for Internet of Things (IoT) based smart health care system is proposed in the paper. From the literature, it is clear that the applications developed using IoT for Healthcare system are to be secured by ensuring user authentication, device authentication, integrity confidentiality and adequate security for data. Many researchers have attempted to give appropriate security with the help of RSA cryptography which are bound to be with limitations such as long time for computation, energy efficiency and long key size. It is proposed that ECC is applied in sensor devices with less memory for the IoT based applications. ECC is recommended for the data encryption because the objects, devices and sensors are very tiny and the heavy weight key exchange will prevent effective functioning[15]. ECC is comparatively more efficient than RSA. So, the security level achieved by RSA with 1024 bit key can be achieved with 160 bit key using ECC [16]. The ECC based security mechanism will address security concerns when deploying or implementing of IoT based Smart Health Services.

III. PROPOSED ARCHITECTURE

The proposed architecture comprises of User Interface, Smart Health service environment and IoT Health Seva Kendra i.e., IoT Information Kendra. The functions of these three units are described below. The security support for proposed architecture is enhanced by adopting various security mechanisms by incorporating ECDSA based certificate, Elliptic Curve Cryptosystems.

A. *Major Componets of the Architecture*

User Interface is a major unit of the proposed Architecture, through which the user can register themselves and the device that is used. The smart health environment is another component from where the raw data of the patients are fetched for further processes of data aggregation and data analysis. The various health sensor devices are connected to the human body i.e., the patients' body. Sesnors and objects are connected to the Smart Readers. Smart Reader is is further connnected to Field Gateway in smart health environment. IoT Health Seva Kendra i.e., IoT Information Kendra is an important unit of the architecture where the data aggregation and analysis take place. The IoT Information Kendra comprises of Smart Gateway, Application Data Server, Application Programming Interface Server, Security Management Server, Data Management Server, Web Services Server and Information Alert Server. Each server has its own roles to play in the architecture. The secured architecture for IoT based Smart Healthcare is depicted in fig 1.

B. *Functionality of the security architecture*

The user has to register the device and the user's credentials to make use of the smart health service provided by IoT Information Kendra. The user credentials such as fundamental biological details, aadhar number and date of birth are obtained from the user and the device details such as IMEI number and mobile number are extracted automatically by User Interface. User id and device id is generated on the device on successful verification of OTP for the same device for the device validation. The User id is generated using username and password by encoding them. Similarly the Device id is generated by encoding the IMEI number and the mobile number registered. A new certificate is generated using User id and Device id. The generated certificate is stored in Smart Gateway and it is validated by the custom certificate validation using the parameters. If the validation is successful, the user and device is registered successfully. To ensure the confidentiality and the information integrity, they are encrypted and digitally signed using Elliptic Curve Cryptosystems. The Smart Gateway chooses a non-singular elliptic curve Ep (a,b) over the finite field GF (p) where p the prime number should be greater than 2^{160}. The points are generated using the point generation algorithm. The generator point G is chosen. Because, the chosen point G has the ability to produce same number of points as the proposed curve. By validating G Private Key (Ptk) is chosen and the Public Key (PuK) is computed.

When a user tries to access the IoT enabled smart service, the encrypted User id and Device id are validated with the information available in the X.509 certificate generated which consists of user information and device information. The user and device's credentials are validated using the User id and Device id. If the credentials of user and user's device match the User id and Device id and the user name and password entered by the user is validated with stored credential in Smart Gateway. If they match, then the user and the device are authenticated to use the IoT based Smart health services. Else, if any one of the above said process fails, the authentication processes terminates and the user or the devices are prevented from using the IoT based health smart service.

To ensure confidentiality, the service providers have to register their service and the IoT devices which are connected to the health service environment. Service credentials like service name and service type are to be registered and based on these a service id is generated. Based on the MAC id or the IP address of the IoT device, IoT Device id is generated. The service providers use Field Gateway at the service environment, to register the service credentials and IoT device credentials with the Smart Gateway. On the successful registration of service and IoT device credentials, service certificate is generated which contains service id, IOT Device id, service type, service name, IP address and MAC id of the Field Gateway. The generated certificate will be validated with the credentials stored in Smart Gateway at IoT Health Seva Kendra. The service and the IoT devices are registered successfully if the validation is successful. The User and Device seek permission when user and device request to avail a smart service. The user is authenticated with the help of the credentials stored in the certificate generated matched with credentials of the user device requesting the service. If they do not match it rejects the user request as the unauthorized access. Secure service authentication ensures the confidentiality and mutual authentication. The encrypted data such as Service id, IoT Device id (MAC Address, IP address) are taken into consideration for the service authentication. When the raw data from the service environment inferred and sent to the IoT Information Kendra via the respective Field Gateway, the Service id, IoT Device id, IP address and MAC id of FG are verified with the credentials of the certificate stored for the respective service. The service is authenticated for further data processing or data aggregation if the credentials of Field Gateway, fetching raw data from service environment with the service certificate match. Else, the raw data fetched from Field Gateway is rejected.

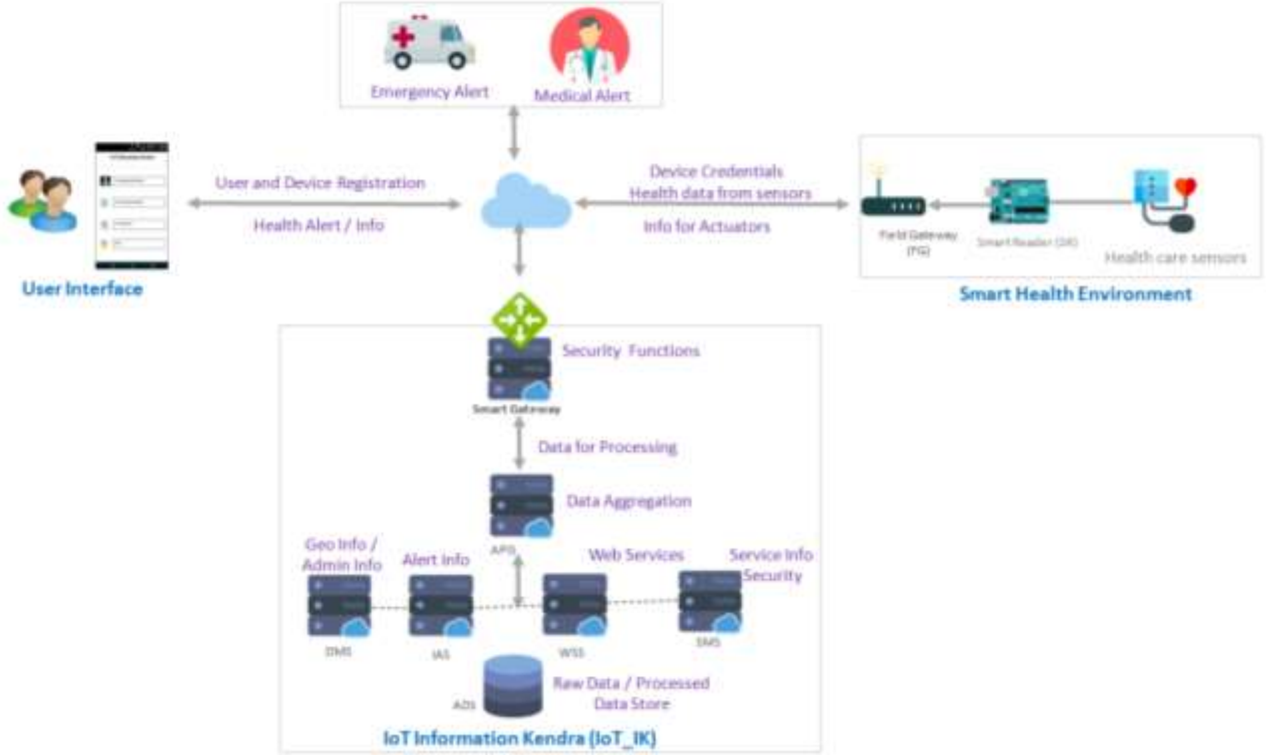

Fig. 1. Secured Architecture for IoT based Smart Healthcare

The health parameters such as blood temperature, BP and pulse rate are inferred from a patient/elderly person through the appropriate sensor devices. The patient's raw data from the sensor are sent or read by Smart Reader. The sensed health parameters of a patient are converted from analog to digital and sent to the Field Gateway using Constrained Application Protocol. The Field Gateway then transfers the inferred data to IoT Health Seva Kendra**.** Smart Gateway validates the service and the health parameters received. On successful authentication of the health parameters of an appropriate registered patient, the authenticated parameters are further to Application Programming Interface Server for data aggregation and analytics based on the algorithms devised. The above said process is carried out in every 5 seconds periodically. If the aggregated data reaches a threshold based the algorithm, the processed information is transferred to Information Alert Server which formulates the processed data into health alerts in different forms.

Information Alert Server sends the alerts to Smart Gateway in which user/patient is authenticated. Once the authentication is accomplished, the health alerts are sent to the needy as coded. Emergency alerts and Medical alerts are sent to Ambulance and appropriate medical staff using the location based information with the help of Data Management Server. Service Providers for Health service are authenticated and authorized appropriately. Hence, the IoT enabled smart health service is fully secured. The privacy of the IoT client's health parameters are ensured by user authentication.

The proposed architecture for Smart health care applications is designed with end-to-end strong multilevel security factors such as confidentiality, mutual authentication, integrity and privacy. The user and device authentication process and service authentication process at Smart Gateway of IoT Health Seva Kendra i.e., IoT Information Kendra to ensure the mutual authentication and other security factors with support of therespective algorithms. The security support for proposed architecture is enhanced by adopting various security mechanisms by incorporating Elliptic Curve Digital Signature Algorithm based certificate, Elliptic Curve Cryptosystems.

Simple ECC based cryptographic method for encryption and decryption is furnished below.

To encrypt the data
i. Sender chooses a random integer 'r'.
ii. Calculates cipher text point using receiver's public key.
iii. C = [(r.G), (M + r. Pu)]
To decrypt the data
i. Receiver multiplies the first point of the cipher text pair (r.G) with the private key (Pr).
ii. Adds this result to the second point of the cipher text pair.
iii. M= (M + r.Pu)-(Pr (r.G))=(M + r.PrG) - (Pr (r.G))
Encryption and Decryption using ECC
The parameters and the variable needed to change the plain text in to cipher text and *vice versa* are:
Pain text taken is Q = 4,433

$Y^2 = X^3 - aX + b \pmod{997}$

a = (-3), b=3

$Y^2 = (-3)^3 + 1 \pmod{997}$

G = Generator Point = (17,427)

Pr = Private Key = 11

Pu = Public Key = (706, 620)

r = Random Number = 7

Cipher Text

C.T = (r * G), T + r*(G.Pr)
= (7*(17, 427)), (4, 433)+7*(706, 620)
= (542, 665), (4, 443) + (482, 299)
= (542, 665), (960,832) = D,2

Cipher text for 'Q" is 'D', '2'

The process in reverse order is adopted to decrypt the plaintext.

Using the private key i.e ('a' * 'pr'), the first point is multiplied

The obtained result is added with the inverse of the second point.

So, Plain Text

PT = b- ('a' * 'pr')
'a'*'pr' = (542,665)*11 = (482,299)
b – ('a' * 'pr') = (960,832) – (482,299)
By adding inverse, the following is obtained
PT = (960,832) + (482,299)
PT = (4,433) = 'Q'

Point doubling, point addition and point multiplication are deployed for this cryptography. Encryption and decryption are more feasible when both the sender and the receiver agree upon the table defined with the chosen elliptic curve. The proposed architecture facilities complete security and enables the users to avail any IoT enabled Health application and services through IoT Information Kendra. It will be more tedious rather difficult for any hacker to hack or break the information during data transmission because of adopting Elliptic Curve Cryptography.

C. *Performance Analysis*

The performance analysis is carried out in a lab simulated environment making used Amazon Cloud services for the IoT based smart health servic proposed. The performance analysis is presented in Table 1. Totally 1000 service requests or service hits have been considered for the performance analysis. The packet drops are recored as 0.2 % and the success rate is 99.8% which is a better result. The bandwidth utilized to complete 1000 requests for the health related smart service is 39.06 Mbps which is very minium. So, the proposed work is proved to have secured IoT based Service.

TABLE I. PERFORMANCE ANALYSIS FOR IOT BASED SMART HEALTHCARE

No. of requests	Packet Drops (%)	Bandwidth Utilized (Mbps)	Success Rate (%)
1000	0.2	39.0625	99.8

IV. CONCLUSION

Healthcare is a major domain for which several research efforts are taken for developing more number of smart applications in secured manner as the healthcare data are more sensitive. Secured architecture IoT enabled health smart services is proposed to materialize the idea of availing IoT based smart health services anytime, anywhere and in any registered device in a secured manner. The proposed architecture is more generic to suit any type of smart health care services and applications. If the proposed work is actualized in real time environment, the IoT based smart health service will be very helpful billions of people in India.

REFERENCES

[1] TRAI, 2015, Technology Digest, Internet of Things. In: Technology Digest, Bulleting of Telecom Technology, Issue 23 July 2015.

[2] Dieter Uckelmann, An Architectural Approach Towards the Future Internet of Things, Architecting Internet of Things - Springer, pp. 1-22 (2011)

[3] Jayavardhana Gubbi a , Rajkumar Buyya b, Slaven Marusic a , Marimuthu Palaniswami, 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 29, 1645–1660.

[4] A Frost, Sullivan, "Smart Cities Need Telecommunications Service Providers: Smarter Solutions provide opportunities to manage resources, create better quality of life", White paper, pp. 1-9, 2016.

[5] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," in *IEEE Access*, vol. 3, pp. 678-708, doi: 10.1109/ACCESS.2015.2437951, 2015.

[6] Ngo Manh Khoi, S. Saguna, K. Mitra and C. Åhlund, "IReHMo: An efficient IoT-based remote health monitoring system for smart regions," *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*, Boston, MA, pp. 563-568, doi: 10.1109/HealthCom.2015.7454565, 2015.

[7] D. F. S. Santos, A. Perkusich and H. O. Almeida, "Standard-based and distributed health information sharing for mHealth IoT systems," *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Natal, pp. 94-98. doi: 10.1109/HealthCom.2014.7001820, 2014.

[8] D. Kwon, M. R. Hodkiewicz, J. Fan, T. Shibutani and M. G. Pecht, "IoT-Based Prognostics and Systems Health Management for Industrial Applications," in *IEEE Access*, vol. 4, pp. 3659-3670, doi: 10.1109/ACCESS.2016.2587754, 2016.

[9] Luliana, I. Chiuchisan, H. Costin and O. Geman, "Adopting the Internet of Things technologies in health care systems," *2014 International Conference and Exposition on Electrical and Power Engineering (EPE)*, Iasi, pp. 532-535, doi: 10.1109/ICEPE.2014.6969965, 2014.

[10] M. P. R. S. Kiran, P. Rajalakshmi, K. Bharadwaj and A. Acharyya, "Adaptive rule engine based IoT enabled remote health care data acquisition and smart transmission system," *2014 IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, pp. 253-258. doi: 10.1109/WF-IoT.2014.6803168, 2014.

[11] Udit Satija, B. Ramkumar and M. Sabarimalai Manikandan, "Real-Time Signal Quality-Aware ECG Telemetry System for IoT-Based Health Care Monitoring," in *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 815-823, doi: 10.1109/JIOT.2017.2670022, 2017.

[12] Vimal Jerald A, Albert Rabara S, Daisy Premila, "Internet of Things (IoT) based Smart Environment integrating various Business Applications", International Journal of Computer Applications, Vol. 128 – No. 8, pp. 32-37, 2015.

[13] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, 2015, pp. 336-341, doi: 10.1109/ICITST.2015.7412116, 2016.

[14] Mikael .A and S. Nadjm-Tehrani, "Attitudes and Perceptions of IoT Security in Critical Societal Services," in *IEEE Access*, vol. 4, pp. 2130-2138, doi: 10.1109/ACCESS.2016.2560919, 2016.

[15] Jiehan Zhou, Teemu Leppänen, Erkki Harjula, Mika Ylianttila, Timo Ojala, Chen Yu, Hai Jin, Laurence Tianruo Yang, "CloudThings: a Common Architecture for Integrating the Internet of Things with Cloud Computing", Proceedings of the 17th International Conference on Computer Supported Cooperative Work in Design, pp. 651-657, IEEE, *ISBN: 978-1-4673-6085-2/13*, 2013.

[16] Daisy Premila Bai T, Albert Rabara S, Vimal Jerald A, "Elliptic Curve Cryptography based Security Framework for Internet of Things and Cloud Computing", Recent Advances on Computer Engineering, WSEAS, pp. 65-74 (2015)