International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Secured Architecture for Integrated IoT Enabled Smart Services

A.Vimal Jerald, S.Albert Rabara, A. Arun Gnana Raj

Abstract*: *Internet of Things plays a significant role in the digital era, as it is to be the game changer in the IT industry. IoT facilitates users with ample number of smart applications and services by connecting billions of devices and objects both physical and virtual. The available IoT based smart services and the applications have its boundaries around a single domain or sector. It becomes tedious when the user wishes to avail different smart services and applications; the user has to request different service providers in various locations for their services. So, it is essential to integrate the IoT enabled services or applications for the user to avail anytime, anywhere and in any device. Security issues are more and different while integrating the IoT smart services by connecting variety of devices and objects. The envisaged security issues must be addressed in the effort of integrating IoT enabled smart applications and services. This paper proposes a novel secured architecture for integrated IoT enabled smart services and applications. The architecture proposed, addresses the integration of IoT enabled services and end to end security using ECC which enables the user to avail IoT services anywhere and anytime.

Keywords* : *Internet of Things(IoT), IoT Smart Services, IoT Security, IoT Security architecture.

I. INTRODUCTION

Internet of Things (IoT) refers to uniquely identifiable objects and virtual representations of the objects in the globally established structure like Internet. The term IoT is used to denote the connectivity of objects, devices, systems and services that goes beyond Machine to Machine Communications (M_2M) and covers of variety of domains, protocols and applications. [1]. IoT is an integrated part of future internet, which could be defined as, dynamic global network infrastructure with self-configuring capabilities based on interoperable communication protocols and standards. Using these protocols, virtual and physical things and object have identities, physical attributes which are connected to internet for processing and to exchange data for communication [2]. In general, IoT is referred to a network of objects using sensors and other related hardware which includes RFID tags, sensors and GPS which can achieve intelligent identification, tracing, and management by data exchange using communication technologies [3].

IoT objects and devices play an important role in business, and society, where they interact and communicate among themselves by exchanging data from environment. They also react real world events and influence the running processes that trigger variety of actions and services without or with human interventions [2]. IoT will foster the development of a number of applications using home appliances, , monitoring sensors, actuators, displays, surveillance cameras vehicles, and many more which make use of the variety of data generated by those objects inorder to provide new services to citizens, business concerns, and to public administrations.[5][6]. The identification, positioning, tracking, monitoring are done intelligently and they are put into applications in various domains [7]. Nowadays IoT has become popular by some of its applications like smart traffic system, electric meter reading, and logistics tracking ect., Different focus groups of Melbourne city have identified Health care, transport, emergency services, defense, crowd monitoring, water quality checking are some of the potential applications of IoT [1]. Existing Internet of Things enabled smart services and the applications under research and development are bound around a single sector or domain. If anyone wishes to avail different smart services or applications, the user has to request different service providers in different locations. Hence, it becomes essential to integrate Internet of Things enabled smart services and applications.

When several objects and things communicate to each other by wireless techniques, there are many security issues such as confidentiality, authenticity, integrity of data inferred from things and human, privacy issue also arise [8]. RFID and sensors are passive and may be easily read by intruders. Enabling encryption protocols and for key storage in the devices with low energy and have no enough power become difficult task. Since all devices have IP address, they can be hacked easily. The access management and device authentication and is also difficult. To ensure confidentiality, a large number of standard encryption techniques are available. But still, the important challenge is to make encryption techniques work faster and less energy consuming. Also, an efficient key distribution scheme should be employed for encryption techniques. Standards need to be devised, to support a wide range of applications in order to address common requirements of industrial sectors, needs of the environment, society at large and the individual citizens [9].

Manuscript published on 30 September 2019
* Correspondence Author
A. Vimal Jerald*, Dept. of Computer Science, St. Joseph's College, Trichy, Tamilnadu, India.
Dr. S.Albert Rabara, Dept. of Computer Science, St. Joseph's College, Trichy, Tamilnadu, India
A. Arun Gnana Raj, Dept. of Computer Science, Bharathiar University, Coimbatore, Tamilnadu, India.

So, it is essential to address these security issues of IoT environment and to put forth proper remedies from an integrated perspective. User and device authentication, services authentication, and information security between IoT infrastructure and core network are the various levels which are focused in this research. The discussed security practices could be envisaged through a Secured Architecture for Integrated Internet of Things (IoT) Enabled Smart Services

II. REVIEW LITERATURE

The review is carried out with the perspective of IoT Smart Applications and Services, Integration of Smart applications and services, and Security aspects of Integrated Internet of things Smart Services environment.

A. Internet of Things Smart Services

Zhao et al. [10] have proposed an application for agriculture called Crop Monitoring System using wireless sensor network. The application is designed by implementing nodes and building sensor networks. The Crop monitoring system has its impact on applications of agriculture IoT. Zhang et al. [11] has coined term Traffic Iot (TIoT). The objective of Traffic IoT is to avoid traffic concession. The number of wireless sensor networks and sensor enabled communications generate IoT of Traffic. The collected information is distributed provided to the user. Compton et al. (2009) [12] have put forth smart health monitoring application to be used for old aged, children and pregnant ladies. RFID enables chips, which are embedded into their bodies to continuously trace the vital health parameters. Nearby health centers will be alerted during the unusual happenings. RFID chips implanted in patients are used to get the medical history of patients and to track the health condition. Sensor technology helps in emergency response and in health care monitoring application.

QI Ai-qin [13] has proposed an application of IoT in Teaching Management System. Key technologies of IoT are introduced as the base for its design and improvement. The study states clearly that the proposed application scheme than the conventional teaching management system. RFID and sensor technology are used for automating the processes of the Departments in the College and for the managerial decision making. The proposal solves the access faults of RFID tag and system security issues by mutual authentication method. Xu Li et al. [14] have proposed an application called smart community extending the smart home application. Controlling applications and monitoring may be feasible via the embedded sensors and actuators, which are remotely controlled remotely in internet. The sensors infer and keep log of user activities, predict their future behavior, and prepare everything one step ahead according to the user's preference or needs, giving the most convenience, efficiency, and security. From the above literature it is clear that the RFID and sensor devices are not equipped with the proper encryption techniques and hence there is no proper authentication of devices.

Tanmay et al. [15] has proposed to integrate the available methodology with latest technologies such as IoT and Wireless Sensor Networks (WSN) for smart agriculture. A newly designed, tested, analyzed an IoT enabled device which is capable of analyzing the sensed data and disseminating the processed data to the farmers. Identification of threats to crops and delivering real time notification based on data processing and analytics.. Martin et al. [16] have dealt the usage of IoT in health and logistics domains. Sensor based quality control in logistics is also discussed. Iuliana et al. [17] have come out with healthcare monitoring system for patients at risk in intensive care units. The system alerts in real time about the change in vital parameters and the movements of the patients and also the preventive measures to the doctors or to the medical assistants. Hong Fong et al. [18] have developed IoT device for traffic management system which collects the traffic flow in real time and communicate to the Microsoft Azure IoT cloud server. The proposed system was implemented on road with BS infrastructure based sensor network using two major systems such as electronic system and software system. The first is comprised of sensors, traffic lights and communication between microprocessor whereas the later includes green light calculation algorithm, cloud server, control system and traffic monitoring application. The above cited research includes both sensor based networks and conventional networks. It has been understood from all the above cited references Security is the major concern in accessing the IoT enabled services. Hence, It has been further studied the security aspects of Integrated IoT enabled Smart Services

B. Security aspects of Integrated Internet of Things Smart Services

CISCO [19] has proposed a IoT security framework which consists of four components which are network enforced policy, secure analytics for visibility control, authentication and authorization. The authentication layer identifies the information of IoT entity using X.509 certificates by establishing trusted relation on identifying the device and connecting the same with IoT infrastructure. The authorization layer controls the access of a device. Only with authorization after authentication establishes a trust relationship between IoT devices to exchange data. The network enforced policy layer consists of the elements which route the traffic securely. The fourth layer defines the services by which all elements in the network infrastructure may participate to provide visibility. It is observed that the sensor devices do not have enough memory to store the certificate or they do not have necessary CPU power to execute the cryptographic operations for the certificate validation.

Bing Zhang et al., [20] have proposed IoT security architecture which consists of perception layer, network layer and application layer. A cryptographic algorithm and protocol are developed light in order to improve physical protection of nodes, secured routing and nodes authentication. The network layer and core layer security are focused to solve security threats and vulnerabilities. Application layer ensures privacy and protection from unwanted access of data.

Lan Li [21] deals with the security mechanisms for the sensor network. It is said that, to construct a complete security framework by integrating different security mechanisms together is necessary to construct secured sensor network. Using the security framework, secured routing, key distribution, encryption mechanisms and intrusion detection will facilitate the integrated security for IoT enabled smart services environment. Don Chen [22] proposes a novel four layered security architecture. Data perception layer emphasizes security measures such as secure routing, intrusion detection and key management. Data integrity and encryption, access security and entity authentication are dealt in network access layer. Kai zhao et al., [23] state that an effective authentication technique should be developed to prevent illegal user interventions, as several applications will have a users at large. It is essential to encrypt RFID signal using the appropriate algorithm to ensure data security of RFID system. This research claims that lighter cryptographic technology can realize confidentiality, integrity and authenticity of RFID system as the RFID devices are with less computational capabilities.

A white paper by Wind River system [24] on IoT security deals with a generic IoT topology. Digital signatures are used on the authorized device to ensure integrity and authenticity. Devices based access control mechanism is extended to network based access control that the information is available to only the area of authorized network. Device authentication for the embedded devices is carried out before the authorization as the machine authentication allows devices to access based on the credentials in the secure storage. Roman et al., [25] deal with network security. From the article it us understood that the heterogeneity of the devices will affect the network. The constrained devices with low bandwidth standard establish communication with more powerful devices such as mobile phones using IEEE 802.15.4. It is learnt that the optimal cryptography algorithm and secure key management system to secure the established communication channel. Bandyopadhyay et al., [26] put forth two major challenges in IoT environment such as privacy and confidentiality. Many standard encryption mechanisms are available to ensure confidentiality. But, the encryption algorithms need to be faster and less energy consuming. Efficient key distribution scheme should be formulated.

Akram et al., [27] stated that the interaction with heterogeneous devices, the user need to authenticate only once using single sign on (SSO) mechanism. It is put forth to adapt existing SSO mechanism or devising new mechanism that is suitable for IoT environment. Though the above literature brings forth security mechanism like digital signature based authenticity, embedded device authentication and cryptographic mechanism for confidentiality, there is a greater possibilities of failures in the cited security mechanisms as the sensor devices used are with less energy for sustaining longer computation and with less space for storage for the cryptographic techniques. Tsao et al., [28] suggest that the security threats and attacks in IoT infrastructure particularly in physical and network layer have to be protected by enabling confidentiality, authentication, availability, access control and integrity.

The existing research on Internet of Things reveals that there is ample number of IoT enabled smart services which work independently. Integrating different IoT enabled services for various applications with adequate security is difficult task and so far no literature cited on Integration of IoT services. Hence, this research article proposes an architecture which integrates the Internet of Things (IoT) enabled smart services and applications. It is clear from the cited literature, IoT infrastructure for integrated smart services environment need to be secured by ensuring user and device authentication, confidentiality, integrity and integrity. Authors have tried out the IoT based services and Security through RSA which is with lot of limitations like long key size, more computational time and less energy efficient. Daisy et al., [29] propose a security framework using Elliptic Curve Cryptography (ECC) for IoT enabled services. Ankita et al., [30] have said that ECC is used widely in constrained devices with lesser memory storage. Moncef et al., [31] have said that ECC is computationally more efficient than RSA and security level by RSA with 1024 bit key is feasibly achieved with 160 bit key using ECC. Elliptic Curve Cryptography is technique to address end to end security concerns in the deployment of IoT enabled Smart Services. The review of literature exposes that, there is no integrated architecture to avail the IoT enabled Smart Services for smart applications. Hence a novel and unique end to end secured architecture for Integrated IoT enabled Smart Services is proposed.

III. PROPOSED ARCHITECTURE

Architecture for Integrating IoT enabled Smart Services

The proposed Architecture for Integrated Internet of Things (IoT) enabled Smart Applications and Services consists of three major units known as the IoT Smart Services Environment, IoT Information Kendra and IoT Client.

A. IoT Smart Services Environment

Senor devices, Smart Readers and Field Gateway are connected appropriately in IoT Smart Services Environment

- **Sensor Devices and Smart Readers**

The sensor devices measure and report the environmental circumstances for information processing and deploying smart applications. The sensor devices are connected with Smart reader using short range wireless radio technology permitting peer to peer communication of devices or GPRS protocols for collecting raw data from the smart service environment. This proposed architecture is experimented with three smart services namely Smart Agriculture, Smart Health Care, and Smart Traffic for the case study.

Soil moisture sensor, Humidity sensor and Temperature sensor are the sensing devices used to infer the signals from the Smart Agriculture environment and the signals are passed onto Smart Reader (SR). The electric signals are converted as the electronic signals transmitted by Smart Reader along with devices identity to the Field Gateway. Similarly, to obtain data for Smart Health Care sensors like

Management Server (SMS) Data Server (DS) Web

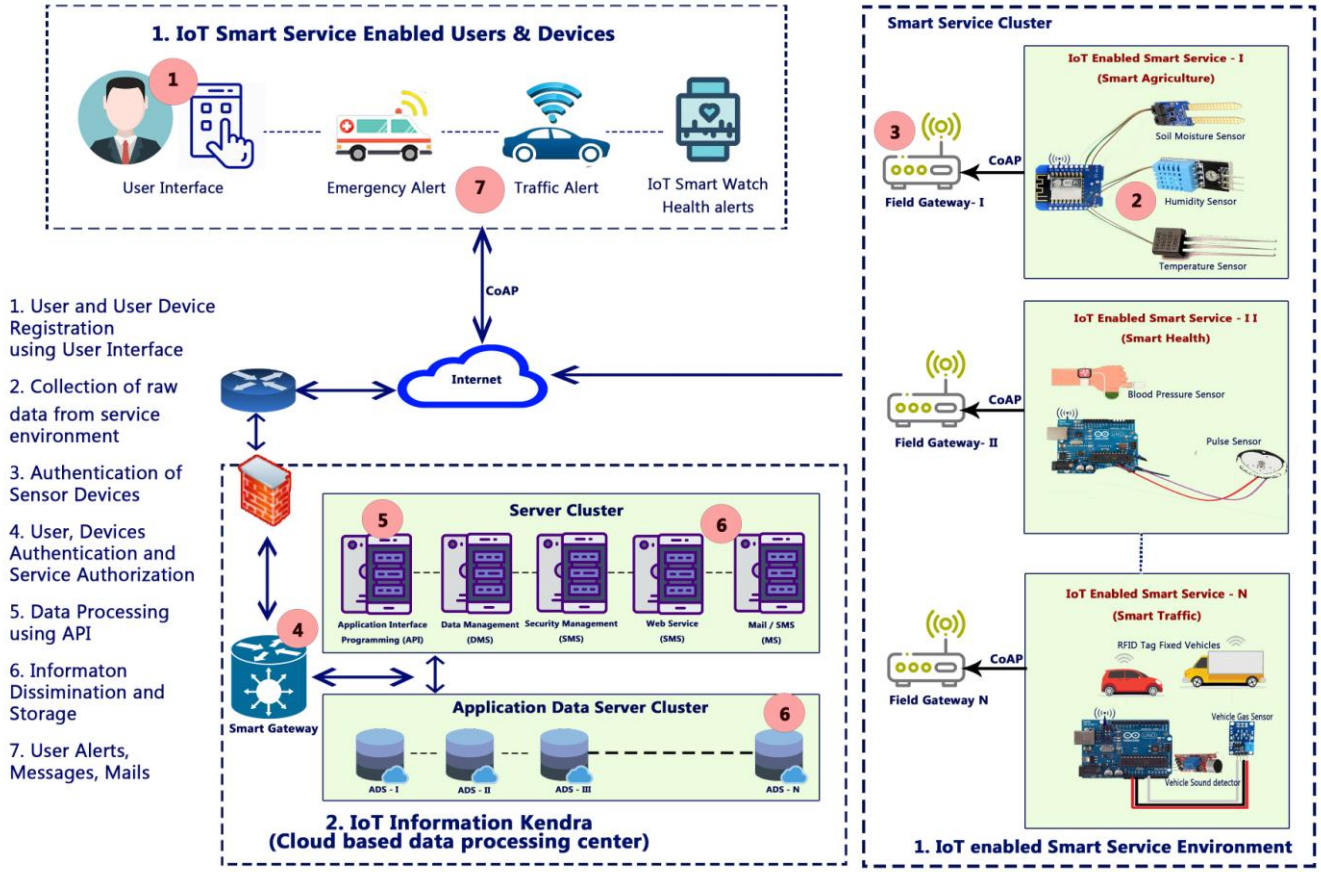


Figure 1. Architecture for Integrated Internet of Things (IoT) enabled Smart Services

heart pulse sensor, blood pressure sensor and body temperature sensors attached to human body gather parameters like heart pulse, Blood pressure, body temperature respectively. The Smart Reader collects the data and sends it to the related Field Gateway. Smart Traffic environment is designed with Vehicle sound sensor, Vehicle detector, Vehicle smoke detector are the few sensors gather raw information from the smart traffic environment. The information gathered is sent to the Smart Reader along with the sensor devices identity and the electronic data is transmitted to the Field Gateway located at the Traffic environment.

- **Field Gateway**

The Field Gateway (FG) connected at the smart services environment is a special server loaded with the smart services applications. The server receives data from the smart environment and transmit the data to the Smart Gateway located in IoT Information Kendra in an encrypted form using Elliptic Curve Cryptography (ECC).

B. IoT Information Kendra

IoT information Kendra is designed for processing and analyzing the data based on the applications suitable for the respective smart services. IoT Information Kendra is designed with different servers like Smart Gateway Server (SGS), Application Programming Interface Server (API Server), Data Management Server (DMS), Security Management Server (SMS) Data Server (DS) Web

security credentials of the Field Gateway and authenticated. This will ensure the user, smart devices and smart services registration and authentication. After completing the verification and authentication, it will forward the data to the API server for further processing of data.

- **Application Programming Interface Server (API Server)**

The API Server will receive the encrypted and authenticated data from the SGS and classify and analysis the data based on the smart services. The API server will send necessary alerts to the user and the registered IoT smart devices, and the related systems. For example, in the Smart Health Care System, depending upon the data, the API server will send alerts to the patient, doctor and the emergency system which are registered and connected. The processed data are frequently uploaded to the Data Server (DS). All the registered smart applications, utilities and tools are stored in the API server. Data Management Server (DMS) will provide the location based GPS data for the smart devices, users and system interconnected.

- **Security Management Server (SMS)**

All the information received from the Smart Gateway Sever and processed by the API server are encrypted with ECC based strong encryption by the SMS server before and after sending the information alert to the user, devices and the connected system.

Strong authentication and certification is also provided by the SMS.

The SMS is responsible for encryption, decryption of processed information. The processed data in the form of alerts, messages, mails or triggers for actuators for the different smart services are disseminated to the user by the Web Service Server (WSS) and Information Alert Server (IAS) which are responsible for the presentation of the information. The SMS also maintains the authentication, authorization, integrity and confidentiality of the registered users, smart devices, Field Gateway and the entire smart systems. The Data Server (DS) maintains the log of all the smart operations and transactions performed in the smart service environment. The proposed architecture for integrating IoT enabled smart services is depicted in Figure 1

C. IoT Client

IoT Client is a hub of users, mobile devices, IoT enabled devices like alarms, Smart Watches, Emergency alerts system, IoT connected vehicles, actuators ect. There is ample number of user devices and each user device may vary and may be based on the Smart Services. The devices may be classified into two. They may be information devices and special purpose devices. Smart Phones, Laptops and Tablets are the information devices which are mainly acting as proxies towards people. These are called people sensors collecting input from people and giving information to people. The special purpose devices are Smart watches, alert systems, sound alarms, switch lights and actuators etc., By the User Registration and Device Registration, the user credentials and the device credentials respectively stored at the SGS of the IoT_IK. All the users, services and devices are registered, authenticated and authorized by the Smart Gateway Server

Secured Architecture for Integrated Internet of Things Enabled Smart Services

The research puts forth a stronger security for the proposed architecture in three levels such as IoT Client Level, IoT Smart Services Environment Level and IoT Data Transaction and Data Processing Level. The three levels of security are corroborated with multilevel authentication using Elliptic Curve Cryptography. The Secured Architecture for Integrated Internet of Things Enabled Smart Services Environment is depicted in figure 2.

A. IoT Client and User Device Level

The security requirements for IoT user and the devices are confidentiality, authentication, privacy and integration. To make the security requirements feasible user and user devices credentials are registered with Smart Gateway (SG) at IoT Data Processing Centre (IoT_IK). ECDSA based Digital Certificates for the devices are generated, stored and verified at Smart Gateway (SG) during user and device authentication to ensure integrity and confidentiality of the data. To ensure privacy of the users, the device authentication is carried out.

B. IoT Smart Services Environmental Level

The sensor devices (SD) at the services Environment (SE) / Field are identified with a device ID each. The devices' IDs are stored with Field Gateway (FG). The sensed data or signals from the devices are received by Smart Reader (SR) is sent along with devices ID and X.509 digital certificate. The device authentication at Field Gateway ensures data collection from appropriate devices. The Field Gateway transmits the collected data to the Smart Gateway (SG) along with MAC ID and IP address of the FG guarantees services authorization.

C. IoT Information Kendra Level

IoT data processing centre named as IoT Information Kendra which plays a significant role in processing of Data for the appropriate application and services. Smart Gateway (SG) at IoT information Kendra which an intelligent node which is responsible for secured data transaction between IoT Information Kendra, Services Environment and IoT Clients and their devices. Security Management Server (SMS) enables the encryption of processed data and public key generation.

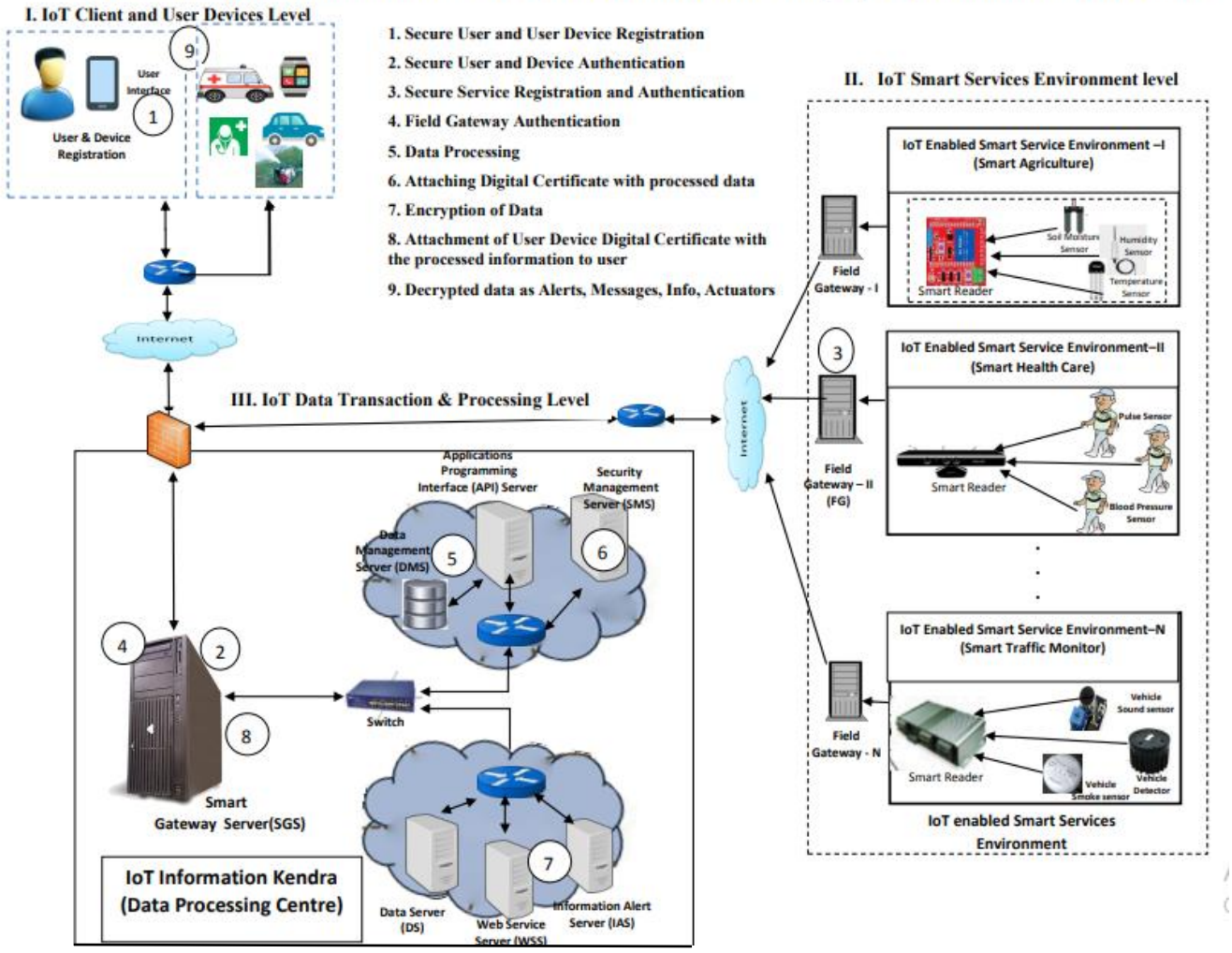
D. Security Requirements

Security requirements are considered with the perspective of confidentiality, integrity, mutual authentication and availability. Mutual authentication is essential between the user, device and services. Mutual authentication should ensure the registered user with registered mobile devices use the appropriate service authenticated. Confidentiality is also a major concern because there may be ample no. of devices and objects of different services dispersed geographically. There is a possibility of intruders accessing the sensor devices in an unauthorized manner to infer the information. The security architecture should ensure the information is prevented from the unauthorized access. Integrity is also equally important like the other concerns. The security architecture should make sure of protecting the information or data from the unauthorized change. It should also guarantee the availability of data to the right person and to the right device.

- **Secure User and Device Registration**

In the User and Device Registration phase the information of the user and the user devices are to be registered with the Smart Gateway of IoT Information Kendra, the data processing centre. The information required for user registration is Name, Date of Birth (DoB), Aadhar Number, Address, Mobile number and E-mail. In addition to that the user creates user name and password. Meanwhile the device details like MAC ID and IMEI number are extracted from the user's device automatically from which the registration is carried out. Upon the receiving the request for registration, the Smart Gateway will send an OTP to verify the user and the device. Once the device is verified a user certificate is generated and the user and device details are stored in an encrypted form using ECC. The key pairs used for encryption and decryption are also generated during the registration. The Smart Gateway at IoT Information Kendra chooses a non-singular Elliptic Curve Ep (a,b) over the finite field GF(p) where 'p' is a prime number and greater than 2^160. It selects a generator point 'G' on Elliptic curve Ep (a,b) as e1 where e1=(x1,y1) and a prime factor 'N' which is largest prime number where NG=0 and N<p. The smart

Figure 2. Secured Architecture for Integrated Internet of Things (IoT) Enabled Smart Services



Gateway randomly chooses a private key pairs where pairs < N and computes e2 =Pairs.e1 where e2 Ɛ Ep(a,b) and computes the public key 'ppk' as Ep (a.b), e1,e2. The public key along with 'G' generator point is at the Smart Gateway whereas the private key 'ptk' is with the user device for the authentication

- **Secure User and Device Authentication**

The proposed security architecture enables the registered the user gets authenticated with the user device registered. Once the registered user, log on using the user name and password which are sent along with the appropriate User and device certificate generated during the registration phase. The Smart Gateway (SG) extracts the user information and validates the user. If there is match of the details extracted and stored, then the device authentication is followed, else the process will be terminated after three attempts. On successful authentication of user, the device is validated using the device information like device_id and U_id are extracted from the device certificate. Once device credentials are validated, the user device is authenticated. If there is a match of user credentials extracted and the stored credentials of corresponding device, the device is authenticated. The mobile app "IoT Information Kendra" is activated and the list of smart services are loaded on the user's mobile device. The user may choose the IoT be terminated and the message is communicated to the user device.

- **Secure Service, IoT Device Registration and Authentication**

The IoT enabled smart services need to be registered with the Smart Gateway (SG) using the Field Gateway (FG). On registration of service name and type of service a service id is generated. MAC address and IP address of the Field Gateway is also stored when the service registration is done. Each sensor device in the smart service environment is assigned an id which is registered with the Field Gateway (FG). A new service certificate x.509 with the credentials embedded is generated using an algorithm based on Elliptic Curve Digital Signature Algorithm. The generated service certificate is stored with Smart Gateway (SG). Service Authentication performed, when the sensor data is collected at Field Gateway (FG) and transmitted to IoT Information Kendra via Smart Gateway (SG). The Smart Gateway receives the encrypted data along with the service certificate and the credentials extracted from service certificate are validated with service certificate stored at the Smart Gateway (SG).

If the credentials stored and received are matched then the data from the service environment is sent to IoT Information Kendra for data processing. If the credentials extracted from the service certificate mismatched with stored service credentials, the Smart Gateway (SG) will cease the data entering into the IoT information Kendra for data processing.

- **Secure Data Transmission between Field Gateway (FG) and Smart Gateway (SG)**

The proposed architecture establishes connection between the Field Gateway and the Smart Gateway after successful authentication between them with the exchange X.509 digital certificate via Transport Layer Security protocol. The Field Gateway (FG) request a connection with Smart Gateway (SG) sends its public using ECC based service certificate X.509. The Smart Gateway checks the authenticity of the certificate. If the signature on the Smart Gateway's certificate matches, then the Field Gateway can be trusted. The session keys are securely exchanged between the FG and SG. The sensor data from the smart service environment can be transmitted securely over this channel.

- **Information Security at IoT Information Kendra**

The inferred data from the sensor device after service authentication, is sent to the the Application Programming Interface (API) and a data log is stored with Data Management Server (DMS). API processes the inferred raw data from the smart service environment based on the application. The processed information is transmitted with key paris generated by the Security Management Server (SMS). The secured processed information from API is sent to the Data Server (DS) for storage. The Web Service Server (WSS) and Mail/Message Server (MS) take care of the presentation of the data using HTTP and SMTP protocols respectively.

- **Secure Data Transmission between Smart Gateway (SG) and the User Device**

The processed data from IoT Information Kendra (IoT_IK) is encrypted at the Security Management Server (SMS) and transmitted to the user device via Smart Gateway. The SG looks for its appropriate device and user certificate based on the control information along with processed data. Once the appropriate the user certificate credentials matched the IoT device credentials, SG routes the data to the appropriate user using the MAC Id of the user device registered. The data is decrypted at the user device using the private key. The data received by the user device may be alerts, messages or mails. In some cases like smart health care the alert messages from IoT Information Kendra reaches the emergency alerts system or a physician making use of the Geographical information supported by DMS.

IV. SECURITY ALGORITHMS

The necessary security algorithms based on ECDSA are devised to make the proposed system more secured. They are secure user and deice registration, secure user and Device authentication, Smart Services Registration, Smart Services verification for posting the data, Encryption and Decryption at the user device. These various levels of security will enhance the proposed architecture secured end to end. The different levels of authentication and proper cryptographic techniques using ECC enable all the tasks such as data processing and data transaction secured between the users, services environment and the IoT Information Kendra. The security algorithms are tested and the performance analysis has been carried out and presented.

V. RESULTS AND PERFORMANCE ANALYSIS

The focus of the experimental study is carried out to test the functionality of the proposed architecture in tune with the algorithms devised. The real time data collection at the service environment is recorded and the results are tabulated. It is also to measure the time taken with respect to user authentication, device authentication, service authentication, hit ratio, system throughput, request response time in terms of encryption and decryption. The performance of the proposed architecture is carried out in a lab environment keeping the discussed criteria as the base. The results simulated are tabulated and presented graphically.

A. Experimental Setup

A test bed in a lab environment is created as the experimental setup for the proposed architecture. The experimental setup involves hardware and software to analyze the performance of the proposed architecture.

- **Hardware/Software Requirements:**

The test bed for the proposed system comprises of of different components like Generic K000007 the Arduino Kit, security gateway, TLS environment and in the cloud platform. Servers with varied configuration are used as smart gateways, security gateway and cloud servers (Amazon m4.Large – instance)

- **Software Requirements:**

The software required for the proposed architecture are IoT Mobile based User Interface, Android development tool kit, open-source Arduino Software (IDE), Parallax Data Acquisition tool, and Elliptic Curve Cryptography package, Open SSL Toolkit and Matlab Tool and Amazon Cloud Services with its AWS.

B. Data Acquisition from Service Environment

Data acquisition from Service Environment is achieved in Smart Agriculture Environment making use of Soil Moisture Sensor Module, Temperature Sensor TMP 45, Humidity Sensor Module SU-HS- 220 and a Generic K000007 the Arduino Kit. This open source Arduino Software is used for flashing the program into the control board. The data from sensors located in the smart agriculture environment is extracted using Parallax Data Acquisition Tool. The Soil moisture, Humidity and Temperature data acquisitioned in excel sheet. The results are given below in Figures 3,4,5,6,7,8

C. Performance analysis

- ***Ping Response Time:***

To analyze the ping response time for the proposed system using ECC, the sample data set for the parallel requesters ranges from 1 to 200 were taken with the increase of 20 requesters. The ping response time graph for ECC is presented in figure 9.

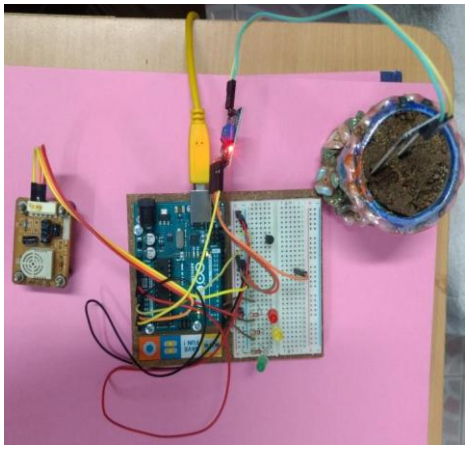


Figure 3. Arduino Generic Kit with Sensors

Figure 4. Arduino Development Kit 1.8.2attached

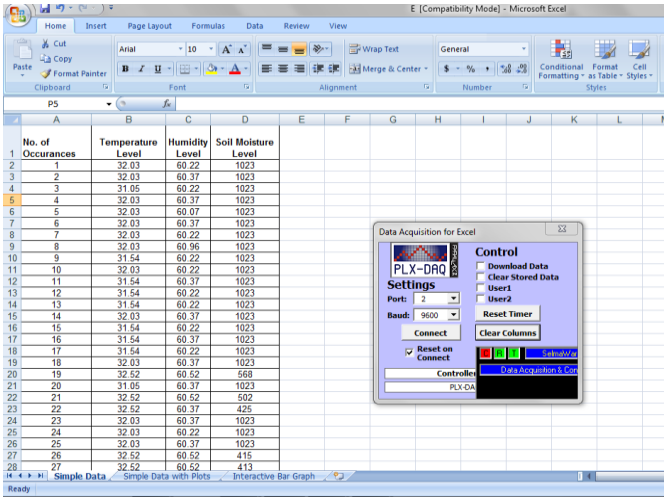


Figure 5. Record Set acquisitioned for Temperature, Humidity and Soil Moisture

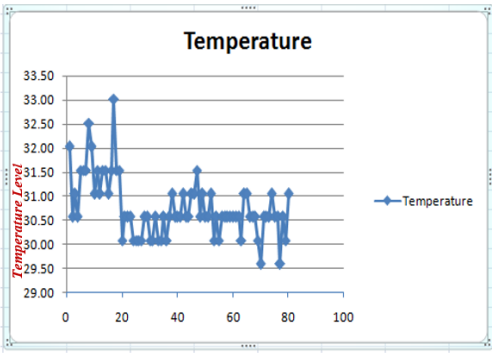


Figure 6. Temperature data recorded

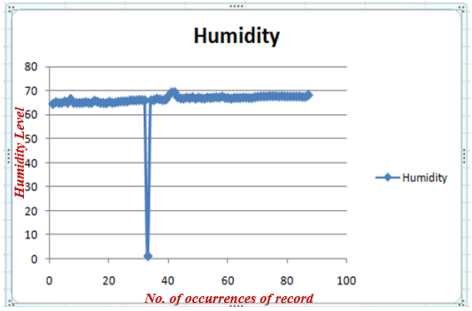


Figure 7. Humidity data recorded

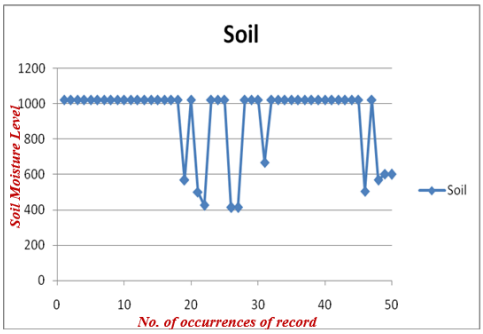


Figure 8. Soil Moisture data recorded

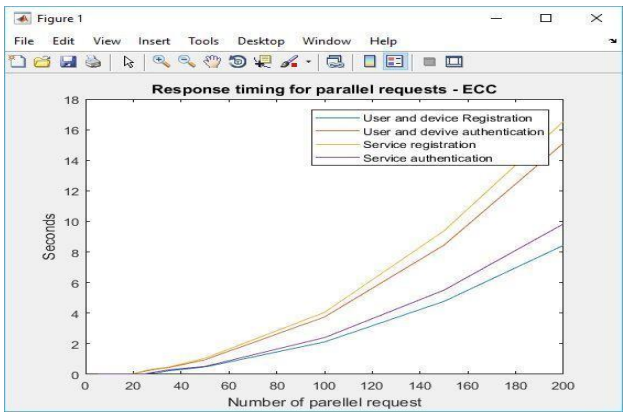


Figure 9. Ping Response time for the security functions 1.8.2attached

▪ *System Throughput:*

Response Timing for Parallel Requests for the Functions	No. of Parallel Requests									
	20	40	60	80	100	120	140	160	180	200
User and Device Registration	0.4643	0.71786	1.04643	1.6643	3.44643	3.84643	4.69976	5.69976	6.69643	7.69643
User and Device Authentication	0.4731	0.74731	1.04731	2.0731	3.74731	4.94731	6.30731	8.30731	15.12231	15.12231
Service Registration	0.5144	0.88858	1.05144	2.9144	4.35144	5.15144	7.52477	9.52477	17.97644	17.97644
Service Authentication	0.4823	0.84823	1.04823	2.20823	3.83823	3.98823	5.71490	6.71490	7.49323	8.49323

Table 1. Response time for various security functions for parallel requests

Response Timing for Processing:

Analysis is carried out to find the response timing for processing User and Device Registration, user and device authentication, Service Registration, Services authentication separately for the response timing for ECC. Time taken for the encryption of the user credentials and device credentials encryption and verification of decrypted values are measured in milliseconds. The results are furnished in the graph (Figure 10).

Security Functions using ECC	Response Timing
User and Device Registration	0.03474
User and Device authentication	0.04723
Service Registration	0.04834
Service Authentication	0.03725

Table 2. Average Response Timing for security functions using ECC

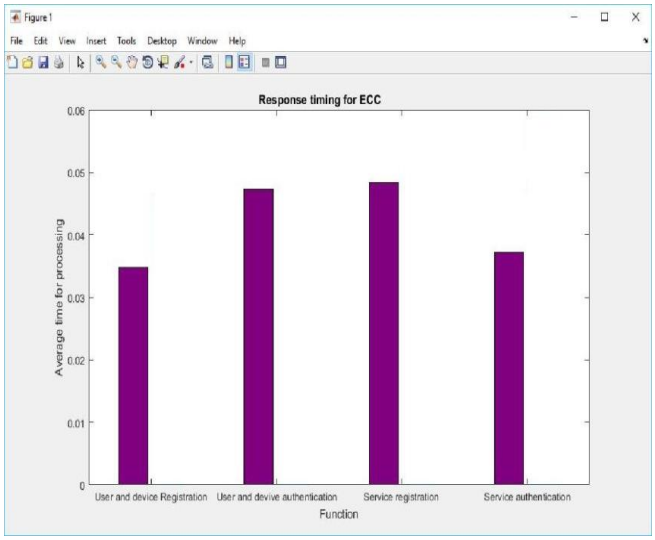


Figure 10. Response Time Processing

The performance test is conducted to estimate the system throughput. It represents the quantum of work, the proposed system does at a stipulated time. Overall system throughput is depicted in figure 11. The system throughput is analyzed for different loads on the server with 10 to 120 service requests. Sample tests have been done with 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110 and 120 services requesters, requesting for the service in the proposed system.

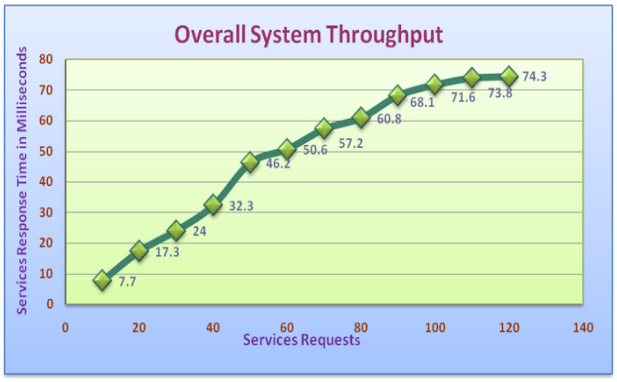


Figure 11: Overall System Throughput

VI CONCLUSION

In this paper, a unique architecture namely A Secured Architecture for Integrated Internet of Things (IoT) Enabled Smart Services has been developed and tested with Generic K000007 the Arduino Kit. The Architecture is fully secured and the end to end security is authenticated with Elliptic Curve Cryptography (ECC). Performance test has been carried out in the field level and the processing level and the results are tabulated. This architecture will be helpful for the common public if implemented in reality. Further, it has to be expanded in diversified areas so as to establish an Integrated Smart city in a secured manner.

REFERENCES

1. Dieter Uckelmann, An Architectural Approach Towards the Future Internet of Things, *Architecting Internet of Things - Springer*, 2011, pp. 1-22.
2. J. Gubbi a , Internet of Things (IoT): A vision, architectural elements, and future directions, *Future Generation Computer Systems* 29 (2013), pp.1645 – 1660.
3. Elkhodr, The Internet of Things: Vision & Challenges, *TENCON Spring Conference, IEEE (2013)*, pp.218-222.
4. Ashton, Internet of Things, *Thing- RFid Journal*, 2009, pp.97-114.
5. J. Jaykumar et.al.,, Secure Smart Environment Using IoT based on RFID, *International Journal of Computer Science and Information Technologies*, Vol. 5 (2), 2014, pp.2493-2496.
6. Lorenzo, Internet of Things for Smart Cities, *IEEE Internet of Things Journal*, Vol. 1, Feb. 2014, pp.22-32
7. TD Division-TRAI, Internet of Things, *In: Technology Digest, Bulleting of Telecom Technology*, Issue 23 July 2015.
8. Elkhodr, The Internet of Things: Vision & Challenges, *TENCON Spring Conference, IEEE (2013)*, pp.218-222.
9. Xie Fang et.al.,, Developing Smart Card Application with PC/SC, *Internet Computing and Information Services, pp. 286 – 289, IEEE*, 2011.
10. Z. Liqiang et.al.,, A Crop Monitoring System Based on Wireless Sensor Network, *Procedia Environmental Sciences 11 (2011)*, pp. 558 – 565.
11. Zhang M. et.al., Smart Transport System Based on The Internet of Things, *Amm. 48-49* (2011), pp. 1073-1076.
12. Comton, M et al., A Survey of the Semantic Specification of Sensor, *proceedings of the 8th International Semantic Web Conference (ISWC 2009), 2nd International Workshop on Semantic Sensor Networks*.
13. QI Ai-qin et.al.,, The Application of Internet of Things in Teaching Management System, *International Conference of Information Technology, Computer Engineering and Management Sciences*, 2011, pp. 239- 241.
14. Xu Li et al, Smart Community: An Internet of Things Application, *IEEE Communications Magazine*, November 2011, pp. 68 – 75.
15. Tanmay et.al., Development of IoT based Smart Security and Monitoring Devices for Agriculture, *6th International Conference Cloud System and Big Data Engineering, IEEE*, pp. 598-602, 2016.
16. Martin et.al., IoT in Practice: Examples: IoT in Logistics and Health, *Enabling Things to Talk, Springer*, Chapter 4, pp. 27-36., 2014.
17. Iuliana et.al., Adopting the Internet of Things Technologies in Health Care Systems, *International Conference and Exposition on Electrical and Power Engineering (EPE 2014), IEEE*, pp. 532-535, 2014.
18. H.F.Chong et.al., Development of IoT Device for Traffic Management System, *IEEE Student Conference on Research and Development (SCOReD)*, 2016.
19. CISCO Security Portal, Securing the Internet of Things: A Proposed Framework http://www.cisco.com/web/about/security/intelligence/iot_framework.html
20. B. Zhang et.al., Security Architecture on the Trusting Internet of Things , *Journal of Electronic Science and Technology*, Vol 9. No. 4, December 2011.
21. Lan Li, Study on Security Architecture in the Internet of Things, *IEEE international Conference on Measurement, Information and Control*, pp. 374-377, 2012.
22. D. Chen et.al., A Novel Secure Architecture for the Internet of Things *Fifth International Conference on Genetic and Evolutionary Computing, IEEE*, pp. 311-314, 2011.
23. K. Zhao et.al., A Survey on the Internet of Things Security , *Ninth International Conference on Computational Intelligence and Security, IEEE CPS*, pp. 663-667, 2013.
24. Wind River Systems, A White paper on Security in Internet of Things, https://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_securityin-the-internet-of-things.pdf , pp. 1-6, 2015.
25. Roman et.al., Securing the Internet of Things, *Article published in IEEE Computer* , vol. 44, no. 9, pp. 51-58, September 2011.
26. Bandyopadhyay et.al.,Internet of Things: Applications and Challenges in Technology and Standardization Springer, *Wireless Press Communication*, pp. 49- 69,2011.
27. Akram, et.al., A Novel Consumer-Centric Card Management Architecture and Potential Security Issues, *Information Sciences* 321, pp. 150-161, ELSEVIER, DOI: 10.1016/j.ins.2014.12.049, 2015.
28. Tsao et.al., Security Threat Analysis for Routing Protocol for Low-power andlossy networks (RPL), Dec. 15, 2013.
29. D. Bai et.al., Elliptic Curve Cryptography based Securing Framework for Internet of Things and Cloud Computing, *Conference on Recent Advances on Computer Engineering by WSEAS*, pp. 65 73, 2015.
30. Ankita et.al., Elliptic Curve Cryptography: An Efficient Approach for Encryption and Decryption of a Data Sequence, *International Journal of Science and Research*, Vol2, No.5, 2013.
31. Moncef et.al., Elliptic Curve Cryptography and its Applications, *Proceedings IEEE International Workshop on Systems, Signal Processing and their Applications (WOSSPA)*, 9th -11th May, Algeria, pp: 247-250, 2011.

AUTHORS PROFILE

A. Vimal Jerald is an Asst. Professor in the Dept. of Computer Science, St. Joseph's College (Autonomous), affiliated to Bharathidasan University, Tiruchirappalli. He is carrying out his research in Computer Science. His area of specialization in research is Internet of Things. He has published and presented research articles in reputed international journals, conferences and seminars.

Dr. S. Albert Rabara is as an Associate Professor in the Dept. of Computer Science, St.Joseph's College (Autonomous), affiliated to Bharathidasan University, Tiruchirappalli. He is one of the pioneers in completing his Ph.D Programme in Computer Science from Bharathidasan University. He is renowned scholar in the field of information technology. He acts as a consultant for institutions and industries. He has a rich experience of 30 years of teaching 20 years of research experience guided more than 10 scholars. He has published more than 100 research articles in reputed Journals, International and National Conference Proceedings. He is serving as a member of editorial board of many International Journals and he is a life time member Computer Society of India (CSI).

A. Arun Gnana Raj is a software architect in Qanawat, Dubai. He is also doing his Ph.D in Computer Science as a part timer, in the Department of Computer Science, Bharathiar University, Coimbatore, India. His area of research is Internet of Things. He has authored many research papers in conferences and seminars in diverse perspectives.