

Minor Research Project - Final Report
(July 2017 – June 2019)

**STUDY ON ESTABLISHING INTERNET OF THINGS
(IoT) BASED INFORMATION KENDRA IN DISTRICT
LEVEL FOR INTEGRATING SMART APPLICATIONS**

(UGC Ref. No.: F. MRP-6559/16 (SERO/UGC) June - 2017)

(Link No: 6559 Comcode: TNBD007 UniqueID: RHTSJC)

Submitted to



UNIVERSITY GRANTS COMMISSION

South Eastern Regional Office (SERO), Hyderabad – 500 001

Principal Investigator

A. VIMAL JERALD, MCA., MBA., M.Phil., NET.,(Ph.D.,)

Assistant Professor in Computer Science



**PG & RESEARCH DEPARTMENT OF COMPUTER SCIENCE
ST. JOSEPH'S COLLEGE (AUTONOMOUS)**

Special Heritage Status Awarded by UGC
Nationally Accredited at 'A++' Grade (4th Cycle) by NAAC
College with Potential for Excellence by UGC
DBT-STAR & DST-FIST Sponsored College

Tiruchirappalli – 620 002



A/c Dy No.	473
Date:	29/06/17

UNIVERSITY GRANTS COMMISSIONS -SOUTH EASTERN REGIONAL OFFICE
 5-9-194, CHIRAG ALI LANE, IV FLOOR, A.P.S.F.C. BUILDING, HYDERABAD -500 001
 Phones: 040 - 23204735, 23200208 FAX: 040 – 23204734, Website: www.ugc.ac.in, email: ugcsero@gmail.com

No.F MRP-6559/16 (SERO/UGC)

Link No:6559.

June,2017

The Accounts Officer
 UGC-SERO, Hyderabad

Comcode: TNBD007
 UniqueID:RHTSJC

30 JUN 2017

Sub: Release of Grants-in-aid to Minor Research Projects for the year 2017-2018.
 Sir / Madam,

The has reference to the Minor Research Project proposal submitted by A VIMAL JERALD Department of DEPARTMENT OF COMPUTER SCIENCE of "St. JOSEPH'S COLLEGE" TEPPAKULAM, TIRUCHIRAPPALLI entitled "Study on Establishing Internet of Things (IoT) based Information Kendra in District level for Integrating Smart Applications". The subject expert, who evaluated the proposal, has recommended for financial assistance as detailed below.

Sl. No	Item	Amount Allocated (Rs.)	Amount Sanctioned as first installment (Rs.)
1.	Books & Journals	40000.	40000.
2.	Equipment	133454.	133454.
	Total	173454.	173454.
3.	Field work & Travel	40000.	20000.
4.	Chemical & Glass Ware	0 0	0 0
5.	Contingency (incl. Special Needs)	40000.	20000.
6.	Hiring Services	40000.	20000.
	Total	120000.	60000.
	Grand Total	293454.	233454.

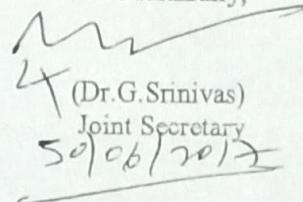
1. I am further to convey the sanction of the University Grants Commission to the payment of Rs.233454. to the principal, St. JOSEPH'S COLLEGE,TEPPAKULAM,TIRUCHIRAPPALLI as first installment (100% Non-Recurring and 50% Recurring grants) towards the above project.

Amount Sanctioned	Head of Accounts	Category
Rs. 173454.	35-CAP-MRP(50)-3(A)2202.03.102.02.01	GEN
Rs. 60000.	31-GIA-MRP(50)-3(A)2202.03.102.02.01	GEN

2. The above approval is subject to the general conditions of grants prescribed by the UGC for this scheme.
3. The sanctioned amount is debitible to the Head of Accounts 35-CAP-MRP(50)-3(A)2202.03.102.02.01 (General), 31-GIA-MRP(50)-3(A)2202.03.102.02.01(General) and is valid for payment during the financial year 2017-18 only and the amount of the Grant shall be drawn by the Accounts Officer (Drawing and Disbursing Officer) UGC-SERO, Hyd. on the Grants-In Aid Bill and shall be disbursed to and credited to "The Principal, St. JOSEPH'S COLLEGE, TEPPAKULAM, TIRUCHIRAPPALLI by Electronic Mode through PFMS Portal at the following details: "(a) Name & Address of Account Holder: The Principal, St. JOSEPH'S COLLEGE, TEPPAKULAM, TIRUCHIRAPPALLI (b) Account No: 137501000020012 (c) Name & Address of Bank Branch: IOB CHINTHAMAN (d) IFSC Code: IOBA0001375.
4. In case the Principal investigator is having ongoing Major/Minor Research Project OR has been transferred/left/retired from the college, the released amount of Rs.233454/- may be returned to UGC-SERO, Hyderabad immediately, failing which action will be initiated against the College for not adhering with the norms of UGC for the scheme.
5. The grantee institution shall ensure the utilization of grants -in-aid for which it is being sanctioned/paid. in case of non-utilization /part utilization, interest @ 10% per annum as amended from time to time on utilized amount from the date of drawl to the date of refund as per provision contained in General Financial Rules of Govt. of India will be charged.
6. The assets acquired wholly or substantially out of UGC's grants shall not be disposed or encumbered or utilized for the purposes other than those for which the grant was given, without proper sanction of the UGC and should, at any time the college ceased to function, such assets shall revert to the UGC.

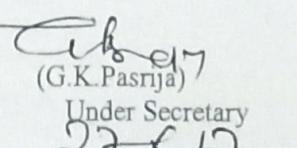
7. The Principal investigator of the project is required to submit the First year progress report of the work done along with the documents 1) Annual Report of the Project as per Annexure-III 2) Utilization Certificate duly signed by the Principal Investigator, Principal & Chartered Accountant 3) Statement of Expenditure for the approved heads for the sanctioned amount as per Annexure-V duly signed by the Principal Investigator, Principal & Chartered Accountant.
8. The interest earned by the College / Institute on this grants-in-aid shall be treated as additional grant which may be shown in the Utilization Certificate / Statement of Expenditure to furnished by the grantee institution.
9. The college has to send the filled in Acceptance certificate within 15 days of receipt of this letter, else the college may return back the sanctioned amount to this office. Further if the conditions of the acceptance letter is not acceptable or applicable to the P.I/College, the sanctioned amount be refunded back to SERO-UGC, Hyderabad.
10. The guidelines of Minor Research Project have to be followed in toto.
11. The Grant is subject to the adjustment on the basis of Utilization Certificate in the prescribed proforma submitted by the University/Institution.
12. The University/Institution shall maintain proper accounts of the expenditure out of the Grants, which shall be utilized, only on the approved items of expenditure.
13. The Utilization Certificate to the effect that the grant has been utilized for the purpose for which it has been sanctioned shall be furnished to UGC as early as possible after the close of current financial year.
14. The college shall maintain a Register of Assets acquired wholly or substantially out of the grant in the prescribed proforma.
15. The College shall fully implement to Official languages Policy of Union Govt. and comply with the Official Language Act, 1963 and Official languages (use for official purposes of the Union) Rules, 1976 etc.,
16. The approval for the above has been received vide letter No.F.7-3/2016(SERO/MRP/RO) dated 6th September, 2016 from UGC, New Delhi.

Yours faithfully,


Dr. G. Srinivas
Joint Secretary
50/06/2017

Copy to:

1. The Principal (Along with DD / Funds transferred through E-mode)
St. JOSEPH'S COLLEGE
TEPPAKULAM, TIRUCHIRAPPALLI - 620002.
A VIMAL JERALD
Dept. of DEPARTMENT OF COMPUTER SCIENCE
St. JOSEPH'S COLLEGE
TEPPAKULAM, TIRUCHIRAPPALLI - 620002.
3. The Dean/Director, College Development Council of affiliating University
4. The Commissioner /Director Collegiate Education, Government of TAMIL NADU
5. The Principal Accounts General (A & E)- Government of TAMIL NADU


(G.K. Pasrija)
Under Secretary
27-6-17

GAR Cap. Sl.No.179. /2017-2018
GAR GIA Sl.No.327. /2017-2018

The sanctioned grant of Rs.233454. /- has been transferred to your college Account as mentioned at the Point No. 3 of this Sanction Order by e-payment through PFMS portal vide date..... You are requested to acknowledge the receipt of the above amount in your account by sending back the enclosed stamped receipt within 7 days.

(R.Rayappa)
Accounts Officer



**UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI - 110 002.**

Proforma for submission of information at the time of sending the final Report of the work done on the project

1. Title of the Project : STUDY ON ESTABLISHING INTERNET OF THINGS (IoT) BASED INFORMATION KENDRA IN DISTRICT LEVEL FOR INTEGRATING SMART APPLICATIONS
2. Name and address of the Principal Investigator : A. Vimal Jerald
Department of Computer Science
St. Joseph's College
(Autonomous)
Tiruchirappalli – 620 002.
3. Name and address of the Institution : St. Joseph's College
(Autonomous)
Tiruchirappalli – 620 002.
Tamil Nadu
4. UGC approval Letter No. and Date : F.NO: MRP-6559/16(SERO/UGC)
dated June 2017
Link No : 6559
Comcode : TNBD007
5. Date of implementation : 20.7.2017
6. Tenure of the project : Two Years
7. Total grant allocated : Rs.2,93,454/-
8. Total grant received : Rs.2,33,454/-
9. Final expenditure : Rs. 2,43,158.40/-
10. Title of the project : STUDY ON ESTABLISHING INTERNET OF THINGS (IoT) BASED INFORMATION KENDRA IN DISTRICT LEVEL FOR INTEGRATING SMART APPLICATIONS
11. Objectives of the project :

This main objective of this minor research project is to design a model for IoT Information Kendra for integrating the various smart applications in district

level, by which to create a smart living environment for general public. Collecting various types of information from many sources of the geographical area of a district and the information to be further processed by IoT Information Kendra. For model, Smart Agriculture, Smart Health and Smart Traffic are the smart services and applications to be integrated with designed IoT Information Kendra. This project enables establishing Internet of Things (IoT) Information Kendra duly supported by the smart environment integrating various applications and domains may be feasible using IoT. Using IoT Information Kendra connected to the smart environment with variety of devices and sensors are facilitate enormous applications and services which will certainly bring significant personal, professional and economical benefits both for the government and for public.

12. Whether objectives were : Yes
achieved

13. Achievements from the project: **Two** Research Article has been published – attached

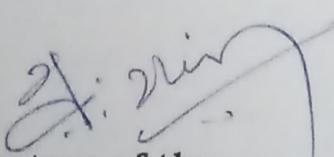
- **A. Vimal Jerald**, Dr. S. Albert Rabara, A. Arun Gnana Raj "Secured Architecture for Integrated IoT Enabled Smart Services", International Journal of Recent Technology and Engineering (IJRTE), Volume-8 Issue-3, September 2019, pp. 7384-7393, (ISBN: 2277-3878). (**Scopus Indexed Journal**)
- **A. Vimal Jerald**, and Dr. S. Albert Rabara, "End to End Secured Architecture for Internet of Things Information Kendra (IoT_IK) Integrating IoT Enabled Smart Services and Application", International Conference on Mobile Computing and Sustainable Information (ICMCSI 2020), Organised by Thirubuvan University, Nepal, 23 January 2020. (Conference Proceedings will be published soon by **EAI/Springer ICC**) (**This research paper was selected as the best paper of the conference**)

14. Summary of the findings : Vide Annexure

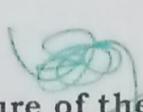
15. Contribution to the society : Vide Annexure

16. Whether any Ph.D. enrolled/ : YES
Produced out of the project

17. No. of publications out of : **Two** Number
the project Attached for kind perusal


Signature of the
Principal Investigator
A VIMAL JERALD
A Group Science
College
Tiruchirappalli - 620002

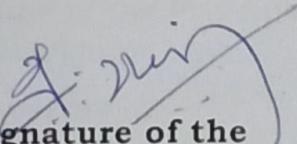



Signature of the Principal
with Stamp
PRINCIPAL
St. JOSEPH'S COLLEGE
(AUTONOMOUS)
TIRUCHIRAPPALLI 620 002

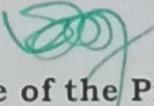
UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI - 110 002

UTILIZATION CERTIFICATE

Certified that the grant of Rs. 2,33,454/- (Two lakh Thirty Three Thousand Four Hundred and Fifty Four) was sanctioned and received from the University Grants Commission under the scheme of support for Minor Research Project entitled **STUDY ON ESTABLISHING INTERNET OF THINGS (IoT) BASED INFORMATION KENDRA IN DISTRICT LEVEL FOR INTEGRATING SMART APPLICATIONS** vide UGC letter F.NO: **MRP-6559/16 SERO/UGC**) and Date **dated June 2017** has been fully utilized for the purpose for which it was sanctioned and in accordance with the terms and conditions laid down by the University Grants Commission.

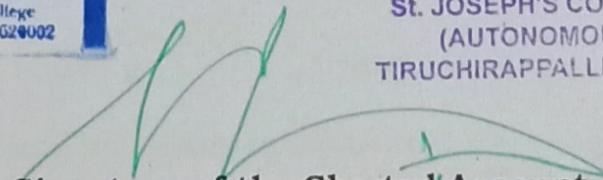

Signature of the Principal Investigator

A VIMAL JERALD
Asst. Prof. of Comp. Science
St. Joseph's College
Tiruchirappalli - 620 002

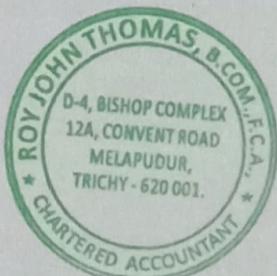

Signature of the Principal with Stamp

PRINCIPAL
St. JOSEPH'S COLLEGE
(AUTONOMOUS)
TIRUCHIRAPPALLI 620 002




Signature of the Chartered Accountant with Stamp

ROY JOHN THOMAS, B.COM., F.C.A.,
CHARTERED ACCOUNTANT
M. No: 200 / 25188



FINAL REPORT OF THE WORK DONE

Title of the Project:

STUDY ON ESTABLISHING INTERNET OF THINGS (IoT) BASED INFORMATION KENDRA IN DISTRICT LEVEL FOR INTEGRATING SMART APPLICATIONS

(UGC Reference No. : F. MRP- 6559/16 (SERO /UGC) June -2017)

CONTENT

1. Introduction

2. Review of the Literature

3. Objectives

4. Methodology

5. Work Completed

5.1. Proposed Architecture

5.2. Functionality of the Proposed Architecture

6. Data Acquisition

7. Result Analysis

8. Feasible Smart Applications

9. Social Contribution

10. Conclusion and Future work

i) References

ii) List of Papers published

iii) Papers Published

FINAL REPORT OF THE WORK DONE

Title of the Project:

STUDY ON ESTABLISHING INTERNET OF THINGS (IoT) BASED INFORMATION KENDRA IN DISTRICT LEVEL FOR INTEGRATING SMART APPLICATIONS

(UGC Reference No. : F. MRP- 6559/16 (SERO /UGC) June -2017)

1. Introduction

New inventions of digital era are real boon to the human kind. Information technology today has made the life style of human beings very smarter. One such technology is Internet of Things (IoT) which is an emerging paradigm that integrates an ample number of smart devices and objects interlinking the physical and the digital world seamlessly. There are varieties of smart applications and services are deployed using Internet of Things. Research and Development units of leading IT industries in India and abroad are working towards the deployment of IoT oriented projects globally. By 2020, there will be the development of mega city corridors and networked, integrated and branded cities. With more than 60 percent of the world population expected to live in urban cities by 2025, urbanization as a trend will have diverging impacts and influences on future personal lives and mobility. Rapid expansion of city borders, driven by increase in population and infrastructure development, would force city borders to expand outward and engulf the surrounding daughter cities to form mega cities, each with a population of more than 10 million. By 2023, there will be 30 mega cities globally, with 55 percent in India.

There are good number of research works are carried out in developing IoT applications like smart agriculture, security and emergency, smart banking, smart surveillances, meteorology, smart health care, smart education, government – e services, smart domestic appliances monitoring, smart traffic, etc. The existing IoT enabled services and applications have its boundary to a single domain or sector. If the user wishes to avail more than one service, may need to approach different service providers and it becomes tedious task. No prominent research has been carried out so far to integrate IoT based smart applications. Hence, it is imperative to design architecture to integrate Internet of Things enabled smart services and applications in order to access

the smart services at anywhere anytime. This minor research project aims to study establishing Internet of Things (IoT) based Information Kendra in District Level integrating smart services and applications. This novel and unique IoT information Kendra to infer and to process the raw data extracted from the various sectors of the smart services environment to facilitate the user with the requested service at anytime, anywhere. This model will certainly help the Government of India to support and enhance the Digital India project. The schemes ‘DIGITAL INDIA’ and ‘SMART CITY’ proposed by Government of India has gained its momentum and because of which IoT is hot research area increasing popularity for industry, government and academia as well. One of the top most initiatives in the form of Digital India Program of the Government which aims at ‘transforming India into digital empowered society and knowledge economy’ is expected to provide the required impetus making use of this minor research project.

2. Review of the Literature

The article by [**Yulongshen et. al., 2017**] have come out a generic IoT architecture supporting two DIY namely network DIY for data aggregation and application DIY for service cooperation. In order to connect these two, a centralized control has been designed to provide standardized interfaces for data acquisition, organization and storage and to support elastic and supportive computing. It is understood from the article that the Micro Things integrate the application environment and the information aggregation environment with the logical centralized controller. The controller connects the two environments which allow interoperation among applications and sensing devices. The article concludes that the micro things consists of data aggregation storage, computing and processing and providing standard interfaces, and hence the architecture unifies fragmented IoT elements into a whole systems, facilitates the control and management of physical devices in the physical world and enriches, the application resources in the cyber world.

[**Tao Zhong et. al., 2015**] have introduced elastic computing framework based IoT architecture. It helps to perform simple operations on data and it will make the data processing or data transformation. It will achieve the capability adaptive deployment of IoT solutions in the form of IoT Applications. Elastic Computing Framework (ECF) based architecture proposed in the

article facilities the flexible operations in solutions that are built upon integration of sensors and actuators of the applications. ECF also enables the agility of front end IoT networks to rich analytics obtained from backend systems. The article makes it clear that the ECF approach benefits building the IoT applications.

This article by **[Dimitrious et. al., 2015]** has presented a vision of a future IoT system architecture that is driven by service discovery. Every layer of IoT service discovery includes on demand discovery and integration of devices, cloud storage and computing storage, computing resources as well as existing data analysis, visualization and application for developing IoT applications. The article makes clear a discovery based IoT solution development mechanism which will enable the users to compare applications that access and process the IoT data without the need to know either the actual source of data, data processing algorithms or infrastructure capabilities.

[Francois carrez et.al.,2017] described an architecture for Federating IoT infrastructure supporting semantic interoperability, based on Architectural Reference Model (ARM) by IoT-A project. The main focus of the architecture is on the paradigm of formulating and managing IoT data from heterogeneous systems and environments and then components like smart devices, sensors and actuators. It also aims at federating large number of test beds across the globe to experiment huge number of semantically interoperable data sources. Raw-data producers, service providers knowledge producers, experimenters are the different stakeholders of the architecture defined. The architecture defined in the article substantiates full-fledged IoT application development with security enhancements.

[Soumya kanti et. al., 2014] have presented their work as IoT architecture that permits real time interaction between mobile clients and sensors and things using a wireless gateway. The architecture is composed of three layers sensing layer containing M2M devices and end points, Gateway API layer and application layer. The wireless gateway acts as the backbone of the proposed architecture. The devices, things and endpoints register themselves in the gateway to be made available to the mobile clients as they are not aware of them. The Necessary API for the discovery phase is implemented in the gateway which is a unique idea proposed in the architecture. The user is enabled with the choice of sensors to receive the measurements which are

represented using SenML. The article concluded that the architecture cited is useful for integrating sensors, actuators, web services and wireless, gateways to deploy IoT M₂M services. **[Souwmya et. al., 2016]** have come out with a framework called Data Tweet enabling data centric IoT services. Data Tweet creates a ubiquitous consumer data service for transmitting short messages for generating actionable intelligence using any computing platforms, to be disseminated to consumers. The article is concluded that the proposed architecture enables data centric IoT services with the consumer interoperability, Data Tweet services and sub systems.

[Yanuarics et. al., 2012] have explored a new concept of extending the functions of IoT objects in order to obtain an integrated and advanced IoT infrastructure by composing an IoT architecture. The architecture initiates brain neural system of living organisms and creating an intelligent framework inspired by human to human interaction as model for machine to machine interactions. The proposed IoT architecture is designed to have different computation level depend on the type of stimuli triggered by the sensing layer. Intelligent process defining the IoT services is centralized on the top of the architecture and intelligent process is distributed to each level of entity in the IoT infrastructure to acquire flexibility for the business process model of IoT implementation.

Zhao et al. 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.** have 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 IoT of Traffic is generated. The collected information is distributed provided to the user. **Compton et al.** have put forth smart health monitoring application to be used for old age persons, infants and pregnant ladies. RFID enables chips are embedded over their bodies to track their vital health parameters. **QI Ai-qin** has proposed an application of Internet of Things in Teaching Management System. Basic concepts and key technologies of internet of things are introduced as the base of its design and improvement. **Xu Li et al.** have proposed an application called smart community extending the smart home application. Using the embedded sensors and actuators are

controlled remotely using internet by which variety of monitoring and control applications may be feasible. **Martin et al.** have dealt the usage of Internet of Things in field of logistics and health. Using smart mobile phones in combination with RFID- or NFC-tagged products provides advantages not only for manufacturers, retailers and customers, but also for delivery and anyone involved in logistical processes for these products

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 prominent Integration of IoT based smart services applications. Hence, this minor research project aims at integrating the Internet of Things (IoT) enabled smart services and applications by establishing IoT based Information Kendra.

3. Objectives

The proposed study aims to design Internet of Things Information Kendra in District level to integrate feasible IoT smart applications and services. The objectives of the project are as follows:

- To study the technical nuances of establishing sensor networks in day today life of human being
- To connect variety of devices and objects to Internet of Things experimentally
- To analyze the feasibilities of establishing Internet of Things based Information Kendra in District level
- To design an architecture for IoT based Information Kendra integrating IoT enabled smart Services covering the geography of a district
- To identify the feasible applications to be integrated to the IoT based Information to enable smart services to general public at anytime, anywhere with any smart devices.

4. Methodology

The aim of this research project is to establish IoT based Information Kendra is to integrate various applications and services to be made available anywhere and anytime for the people of rural and urban India. The various

means of sensor nodes are to be networked to create smart services environment. An architecture is to be designed to integrate IoT based smart services and applications by IoT information Kendra. Technical aspects of establishing IoT Information Kendra along with necessary mechanisms are to be devised. The cloud servers' support for the IoT information Kendra are to be studied. The feasible applications are to be identified which are more benefitting general public. Case studies with few feasible applications in the simulated environment are to be examined. Feasibility study is to be made by establishing IoT based Information Kendra in district headquarters, so that the Information Kendra provide the data or necessary services anytime, anywhere and with any registered devices.

5. Work Completed

Phase 1: Technical study of sensor devices and sensor networks are done

Phase 2: An Architecture is proposed to integrate the IoT based Smart Services and applications by establishing IoT information Kendra

Phase 3: Feasible IoT based smart applications and services are identified

Phase 4: Designed an User Interface (UI) for User and Device Registration

Phase 5: Test bed has been designed based on the proposed architecture

Phase 6 : Data Acquisition and Result Analysis

5.1 Proposed Architecture to Establish IoT Information Kendra

The proposed Architecture establishing IoT Information Kendra to Integrate IoT Enabled Smart Services is envisaged to integrate variety of IoT enabled smart services and applications avail the IoT enabled smart services anywhere, anytime and any smart device.

The architecture integrates 1 to N IoT enabled smart services using internet as backbone and the smart services and applications are deployed in cloud environment known as IoT Information Kendra (IoT_IK) using Smart Gateway (SG). Sensors, Smart Readers (SR) and Field Gateway (FG) create IoT enabled Smart Services Environment (SSE). User's device with user interface and IoT enabled devices make IoT client. The Smart Gateway acts as the interface between the IoT SSE and IoT Client. IoT_IK aggregates the sensed data from

the smart service environment and issues the alerts or messages or commands to the actuators of IoT enabled devices. The architecture is depicted in figure 1.

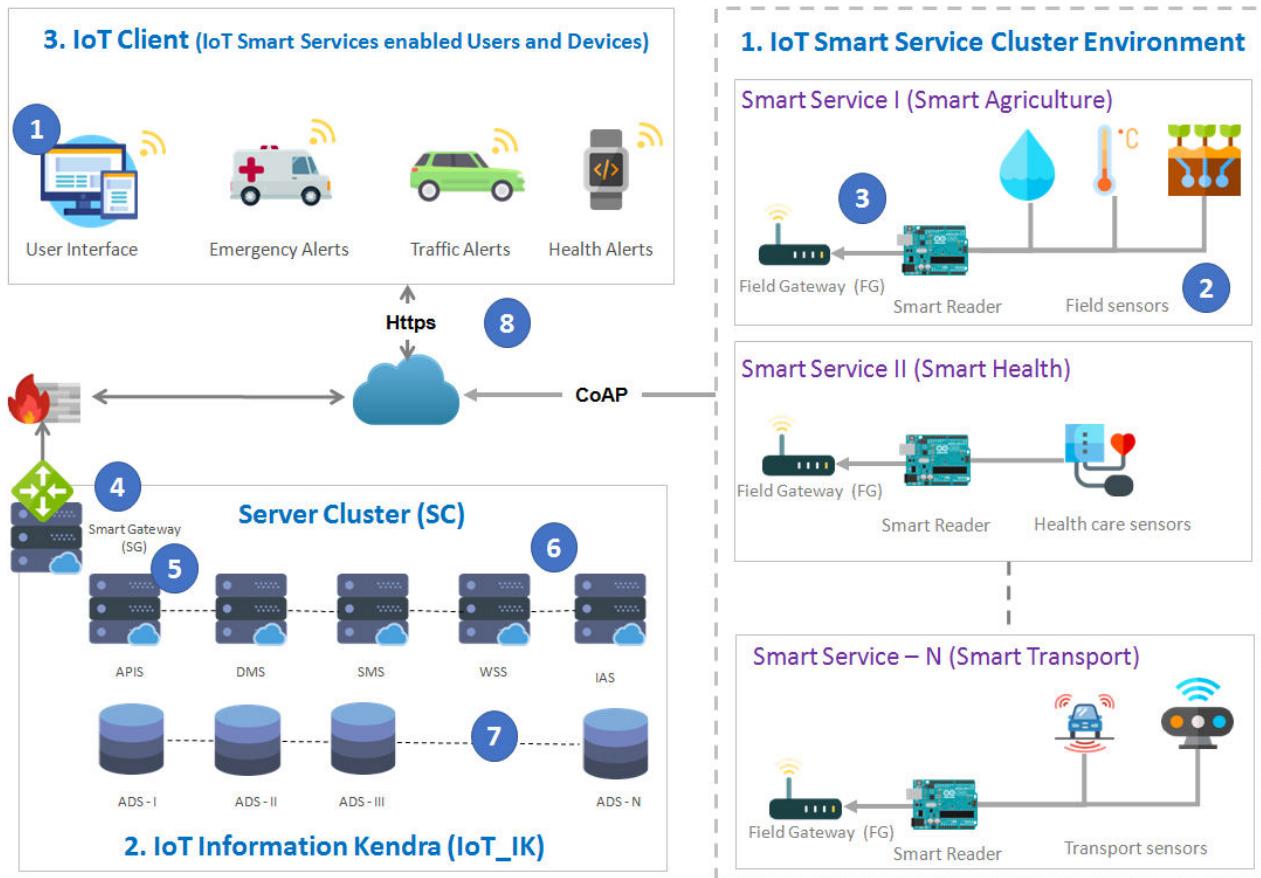


Figure 1. Proposed Architecture

Sequential Processes in the architecture

1. User and Device Registration using User Interface (UI)
2. Inferring raw data from Service Environment
3. Authentication of Sensor Devices Smart Readers
4. User, Device Authentication and Service Authorization
5. Data Aggregation using APIS
6. Information Dissemination
7. Data Store
8. User Alerts/ mails/ messages

Major Components of the Proposed Architecture

The proposed Architecture consists of three major units known as the IoT Smart Services Environment, IoT Information Kendra and IoT Client. The functions of all the three units are presented below.

a) IoT Smart Services Environment (SSE)

IoT Smart Services Environment (SSE) consists of Sensor Devices, Smart Readers (SR) and Field Gateway (FG) which are connected appropriately in IoT SSE. The raw data are collected for the aggregation of data and thus for the deployment of IoT smart services and applications using Application Programming Interface Server (APIS). The components of IoT SSE play a vital role and the detailed report of each component is given below. The IoT Smart Services Environment is depicted in Figure 2

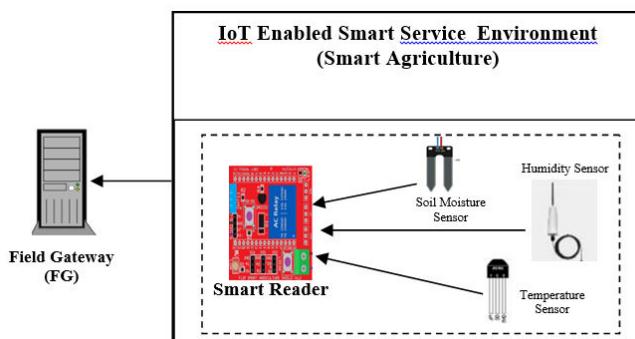


Figure 2. : IoT Smart Service Environment

Sensor Devices and Smart Readers

The sensor devices infer 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 for collecting raw data from the smart service environment. SR collects the sensed data in the form of analog signals or digital signal. In case of analog signal, the SR converts the analog signals into digital data. 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 and Humidity senor is depicted in Figure 3. a and Figure 3. b 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 SR. The electric signals are converted as the electronic signals transmitted by Smart

Reader along with devices identity to the FG. Similarly, to obtain data for Smart Health Care sensors like 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 respective FG. Smart Traffic environment is connected with Vehicle sound sensor, Vehicle detector, Vehicle speed detector which are the few sensors gather raw information from the smart traffic environment. The information gathered is sent to the SR along with the sensor devices identity and the electronic data is transmitted to the FG located at the Traffic environment. The data communication between the constrained devices of SSE, FG and IoT_IK using Constrained Application Protocol (CoAP) which is suitable for constraint devices and for the constrained networks. Arduino Control board performs the role of SR which is depicted in the Figure 3. c



Figure 3.a : Soil Moisture Sensor

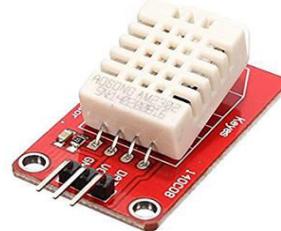


Figure 3. b : Humdity Sensor



Figure 3. c : Smart Reader (Arduino Kit)

Field Gateway (FG)

The Field Gateway (FG) at the SSE is a special server connected to the SR. The details of the sensor nodes and the SR are registered at the time of installment for the purpose of sensor devices' identity. The FG receives data from the SSE inferred by the sensor devices. The received data along with the control information is transferred via Internet using CoAP to the Smart

Gateway located in IoT_IK in an encrypted form. The control information consists of the MAC id of FG and the identity details of the Sensor Nodes. Each SSE in the Smart Service Cluster Environment will be connected to a FG separately which communicates rather transfers the raw data from SSE to IoT_IK for data aggregation.

Smart Service Cluster Environment (SSCE)

The Smart Service Cluster Environment (SSCE) may comprise of 1 to N IoT enabled smart applications and services. Each Smart Service Environment (SSE) is connected with a Field Gateway (FG). Service cluster is also known as IoT enabled smart services environment. FG establishes communication with SG of IoT_IK. The Smart Service Cluster Environment is depicted in figure 4.

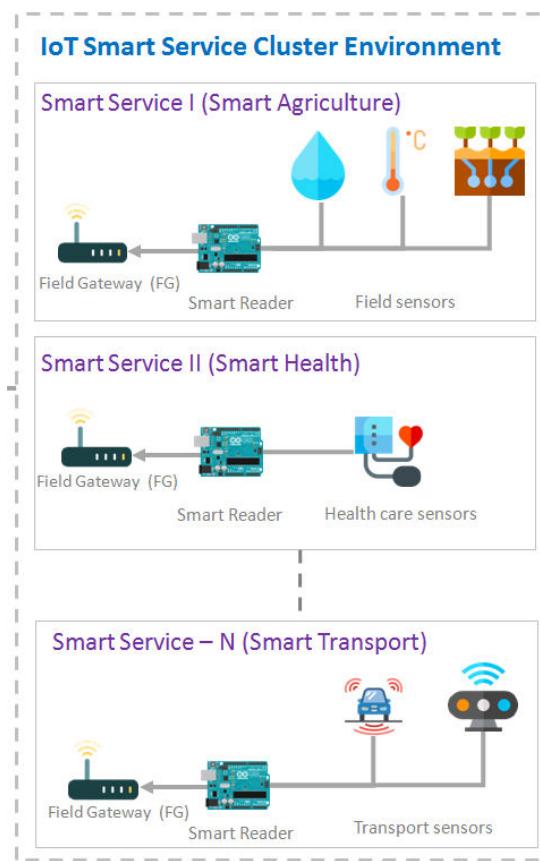


Figure 4. : Smart Service Cluster Environment (SSCE)

b) IoT Information Kendra (IoT_IK)

IoT information Kendra (IoT_IK) is designed for processing and analyzing the data based on the applications suitable for the respective smart services. IoT_IK comprises of Server Cluster (SC), Application Data Server Cluster (ADS), and Smart Gateway (SG). IoT_IK is a cloud based data processing

center which suits IoT enabled smart services and applications handling huge data 24 x 7 basis. IoT_IK is depicted in figure 5.

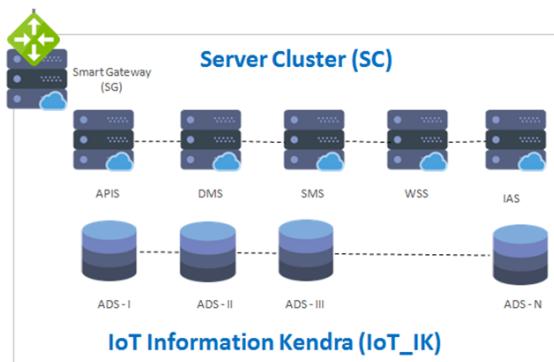


Figure 5. : Internet of Things Information Kendra (IoT_IK)

Server Cluster (SC)

The Service Cluster (SC) in IoT_IK comprises of different servers such as Application Programming Interface Server (APIS), Data Management Server (DMS), Security Management Server (SMS), Application Data Server (ADS), Web Services Server (WSS) and Information Alert Server (IAS). Since the volume of data inferred from the SSE is huge; there is a Cluster of ADS to accommodate the data processed. All these servers are configured in a cloud environment which can be accessed from anywhere, anytime and any registered device. The Server Cluster is responsible for data aggregation in a secure manner. Each server plays its role over the data aggregation or data analytics for realizing the IoT based Smart Applications. Server Cluster is depicted in figure 6.

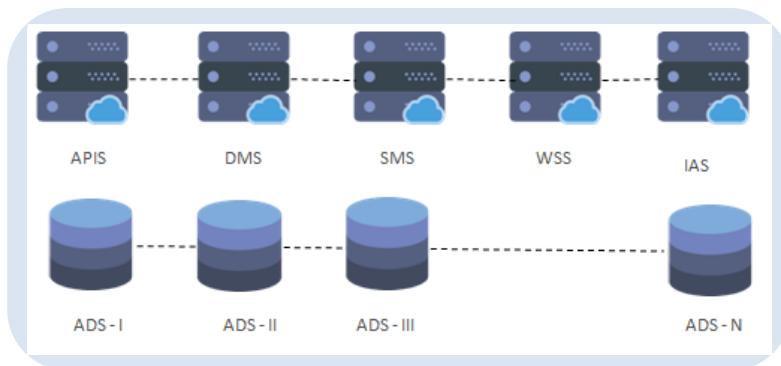


Figure 6. : Server Cluster

Smart Gateway Server (SG)

The Smart Gateway Server (SG) receives the data from the Field Gateway (FG) in an encrypted format. SG will verify all the security credentials of the FG

and authenticate the credentials of FG and the IoT devices at SSE before the data is transmitted to IoT Information Kendra (IoT_IK) for data aggregation or for data processing. SG facilitates the user, smart devices and smart services registration and authentication. Accomplishing the verification and authentication, SG forwards the data to the APIS for further processing of data based on application based algorithms. SG acts as the interface between the SSE, IoT client and the IoT_IK

Application Programming Interface Server (APIS)

The Application Programming Interface Server will receive the encrypted and authenticated data sent from the SGS. The raw data from SGS is decrypted at APIS and the data is classified and analyzed using the predefined programs and algorithms based on the IoT enabled smart services or applications. The APIS 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 aggregated information, the API server will send alerts to the patient, doctor and the emergency system which are registered and connected. All the registered smart applications, utilities and tools for data analysis are stored and installed appropriately in the APIS.

Application Data Server (ADS) and Data Management Server (DMS)

The processed data are periodically uploaded to the Application Data Server (ADS). The ADS is responsible for keeping the log of data processed for a particular period of time. ADS requests the assistance of Data Management Server (DMS) to provide location based details when there is need for users alert on an abnormal condition detected. The DMS analyzes and extracts the location based Global Positioning System (GPS) data for the smart devices, users and system interconnected for disseminating the message alerts. DMS is enabled with GPS location identifier based on the inferred data from the SSE. For example, when the health condition of patient is critical, the GPS location of the patient will be detected by DMS and an alert message will be sent to a Doctor, Emergency Service Alerts and the hospital near the patient's location.

Security Management Server (SMS)

All the information received from the SG and processed by the APIS are encrypted using ECC based strong encryption after proper authentication. The SMS generates and stores the SSL certificates before and after sending the information alert to the user, devices and the connected system. The user alerts or messages sent to the user along with ECDSA based certificate which ensures the security factors such as integrity and confidentiality. 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, FG and the entire smart systems. The ADS maintains the log of all the smart operations and transactions performed in the SSE.

Web Service Server (WSS) and Information Alert Server (IAS)

The processed information is disseminated to the user in the form of mail or message alerts using Information Alert Server (IAS). Web Service Server (WSS) is responsible for presentation of processed data for the web based applications using Hyper Text Transfer Protocol (HTTP) if there is a need. The presentation formatting and content management based on the Users devices are carried out by WSS whereas the IAS is responsible for presentation of message formatting based on the smart applications and services.

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 etc., There is ample number of user devices and each user device is heterogeneous in nature and may be based on the Smart Services. The devices may be classified into two which are information devices and special purpose devices. Smart Phones and Tablets are the information devices called as 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 **SG** of the **IoT_IK**. All the users, services and devices are registered, authenticated and authorized by the **SG**. The IoT client is depicted in Figure 7.

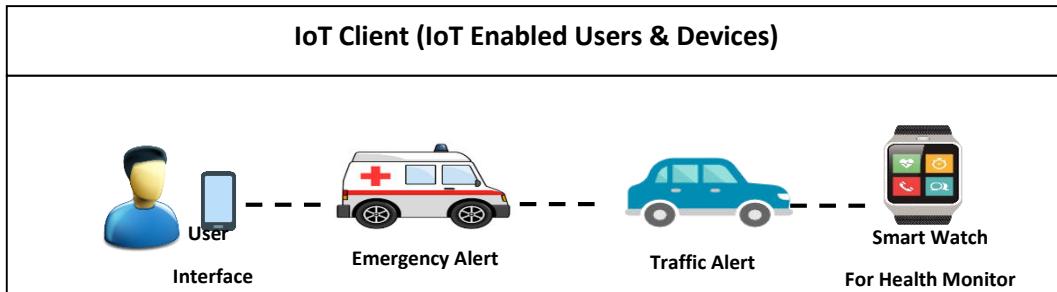


Figure 7. IoT Client

5.2. Functionality of the Proposed Architecture

The proposed architecture enables the integration of IoT enabled smart services and applications and facilitates the user to avail the IoT services securely anytime, anywhere and with registered device. The user establishes a connection with Smart Gateway (SG) at Internet of Things Information Kendra (IoT_IK) using Hyper Text Transfer Protocol (HTTP) via internet. The user with the help of User Interface (UI) at the user's device requests the SG for the secure user and user device registration. The user through UI feeds the user details such as name, DoB or age, aadhaar number, mobile number and email id. The user device credentials such as MAC id or IMEI and IP address are extracted automatically. User is primarily authenticated using OAuth at SG by sending a One Time Pin (OTP) to the mobile number entered by the user for the primary verification. On successful verification of mobile number, User id (U_id) and Device id (D_id) are generated by the SG using user and Device credentials. Certificate registry at SG generates the user certificate based on ECDSA by encrypting U_id and D_id using ECC. Key pairs such as Public Key (PuK) and Private Key (PtK) are also generated using ECC cryptosystem. The generated user certificate is stored in certificate registry at SG along with PuK. The same user certificate is sent to the user device along with PtK for further authentication.

The sensor devices, objects and Smart Readers (SR) at at Smart Service Environment (SSE) are registered with the corresponding Field Gateway (FG) of SSE. The sensed raw data by the sensor devices are read by Smart Reader

(SR) and the same is sent further to the FG. A network communication is established between FG and SG of IoT_IK using Constrained Application Protocol (CoAP). FG using the UI, requests SG for service registration. The service credentials such as service name, service type, IoT Devices id allocated by FG, MAC id and IP address of FG are used to generate S_id and IoTD_id after fundamental authentication using Oauth at SG. Certificate registry at SG generates a service certificate using S_id and IoTD_id along with PuK and PtK generated using ECC. The service certificate generated is stored in the certificate registry along with its PuK. The same certificate is sent to FG along with PtK.

The raw sensed data from SSE are sent by FG along with the corresponding service certificate is sent to SG using CoAP over the established connection between FG and SG. The service is authenticated securely at SG using credentials in service certificate with the stored credentials at certificate registry. The PuK at SG and PtK are sent by FG are used to decrypt the data in the certificate. On successful authentication, the sensed data are sent by FG are further sent to Application Programming Interface Server (APIS) for data analysis.

The sensed data is received at APIS at a fixed time interval after the secure authentication of services. APIS aggregates and processes the data based on the service using the respective algorithms. Data Management Server (DMS) supports the APIS with the GPS information and other information related the SSE. Web Service Server (WSS) helps the APIS with web based services on demand to supplement data processing. The processed data are stored at Application Data Server (ADS) regularly. If the processed data reaches a threshold state based on the algorithm, the data is to be sent to the IoT client as alerts or messages. Information Alerts Server (IAS) facilitates APIS for message formatting based on the IoT client. The Security Management Server helps encrypting the alert information with the help of ECC cryptosystem. The encrypted form of alerts and messages to IoT client are sent with PuK from SG. The PuK is sent along with the message or alert and the PtK with the user or IoT client will decrypt the data. Hence, only the appropriate user or IoT client will receive the alerts or messages securely.

When the user requests SG at IoT_IK for a service using UI at the user's device, the service certificate is sent along with the PtK, SG will validate the credentials in the certificate decrypted by respective PuK. The secure user and device authentication is carried by matching the credentials of the certificate and the credentials stored at certificate registry. On successful authentication, the user request is further sent to APIS for the requested data. APIS in turn processes the request and with the help of other servers of Service Cluster (SC) at IoT_IK. SG establishes a secure communication between IoT_IK and IoT client or the user device using HTTP. The requested service information is sent to the user or to the IoT client through SG. The service information in an encrypted form with PuK is sent to the user's device. The user device with the help of PtK decrypts the data. So, it is possible only for the appropriate user device to receive the requested service information securely.

6. Data Acquisition

Data acquisition from Service Environment (Smart Agriculture) is achieved in simulated experimental setup with the help of Arduino Uno Rev3 by making use of Soil moisture sensor module, Temperature Sensor, and Humidity Sensor Module. Open source Arduino Software is used for flashing the program into micro controller. The data from the service environment is inferred using Parallax Data Acquisition Tool. The soil moisture, Humidity and Temperature data acquisitioned in excel sheet for the interval of 5 seconds. The data inferred are given below in figures 8.1, 8.2, 8.3, 8.4, 8.5, 8.6.

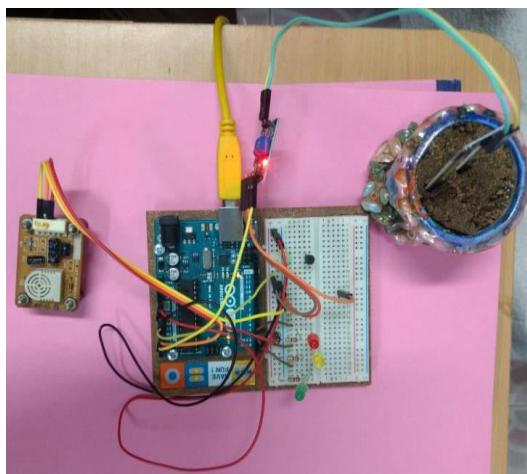


Figure. 8.1: Experimental setup for data acquisition



```

smart_Agri | Arduino 1.8.2
File Edit Sketch Tools Help
smart_Agri
void setup() {
  // put your setup code here, to run once:
  Serial.begin(9600);
  Serial.println("CLEARDATA");
  Serial.println("LABEL,Time,Temperature,Humidity,Soil");
}

void loop() {
  // put your main code here, to run repeatedly:
  Serial.print("DATA,TIME,");
  int sensorVal = analogRead(A0);
  //Convert reading to voltage
  float voltage = (sensorVal/1024.0) * 5.0;
  //convert millivolts into temperature
  float Temperature = (voltage - 0.5) * 100;
  float Humidity=((5.0*analogRead(A1)/1024)/0.033);
  int Soil = analogRead(A2);
  Serial.print(Temperature);
  Serial.print(",");
  Serial.print(Humidity);
  Serial.print(",");
  Serial.println(Soil);
  delay(10000);
}

```

Done uploading.

Figure 8.2: Arduino Software Development Kit

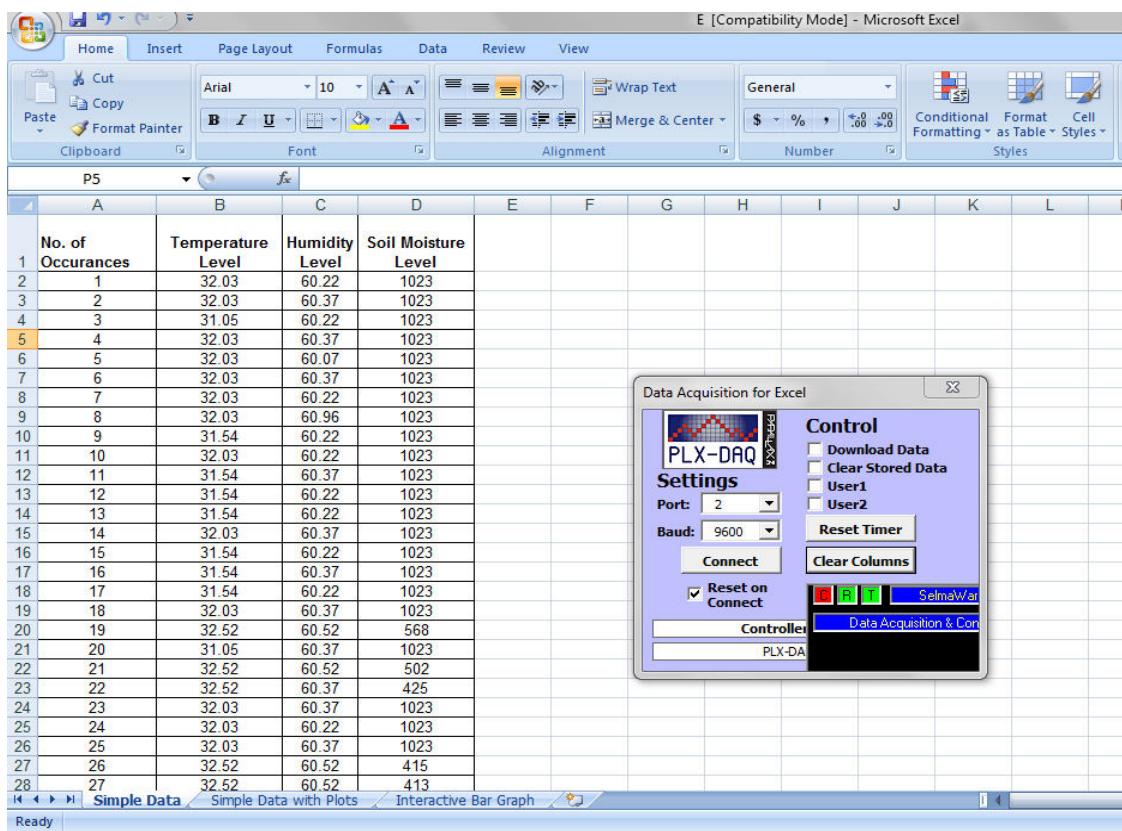
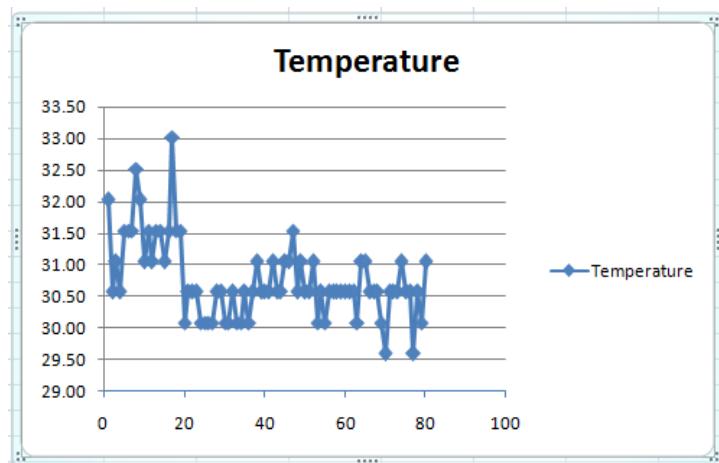
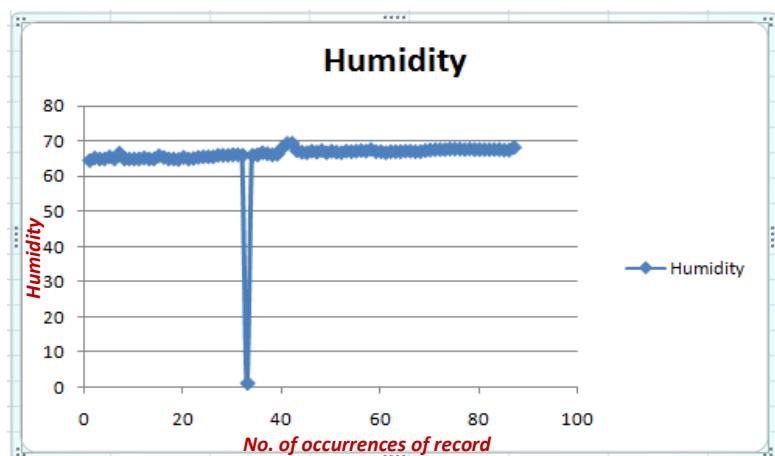


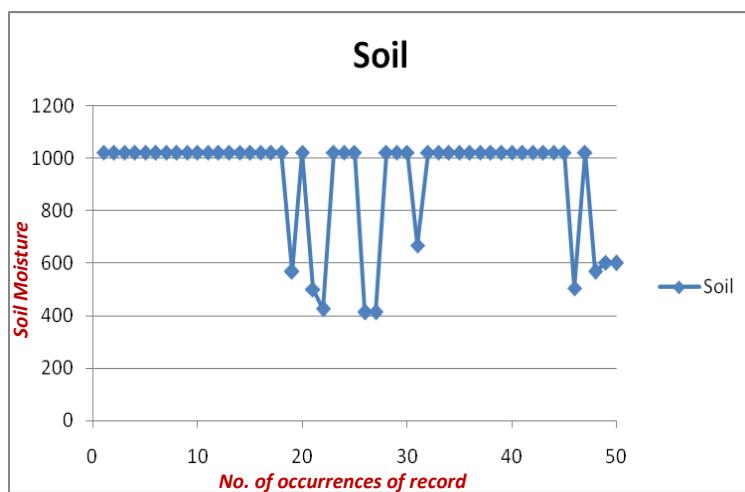
Figure. 8.3: Record set acquisitioned for Temperature, Humidity and soil moisture



8.4: Temperature record set inferred



8.5: Humidity record set inferred



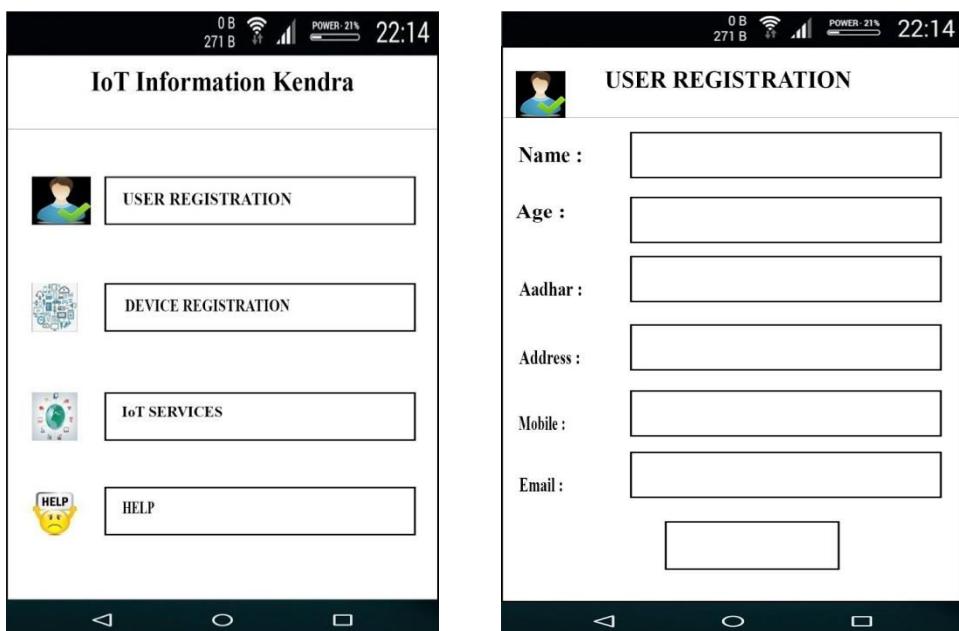
8.6: Soil Moisture record set inferred

7. Result Analysis

Performance Analysis on User and Device Registration

The user and device registration is carried out securely making use of the security algorithm proposed for the same. The user and device registration is

done using User Interface depicted in figure 9. User credentials such as Name, age, aadhaar number, mobile number and email id are fed into SG using UI. The device credentials such as IP address and MAC id are automatically extracted from the device used by the IoT client. U_id and D_id are generated by SG and a self-signed certificate using ECDSA is created. The registered information is encrypted using ECC using the key generated by ECDSA. Among thousand parallel requests, 200 requests were chosen and analyzed with the interval of 20 requests. The response time taken and memory consumed for secure user and device registration for the obtained sample graphically represented in Figure 10. and Figure 11. respectively.



9: User Interface for user and user device registration

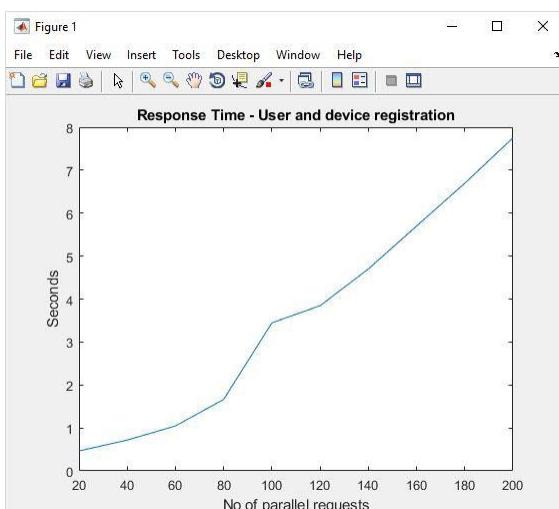


Figure 10: Response time

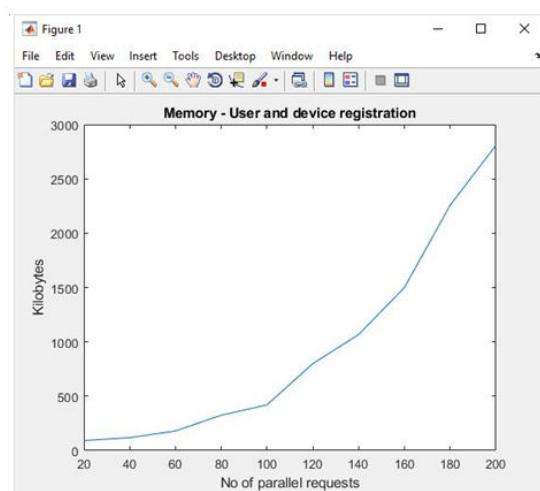


Figure 11: Memory Consumed

Table 1. Response time and Memory consumed for User and Device Registration

Response Timing for Parallel Requests for the Functions	No. of Parallel Requests									
	20	40	60	80	100	120	140	160	180	200
Time Taken in Seconds	0.464 3	0.71786	1.04643	1.6643	3.44643	3.84643	4.69976	5.69976	6.69643	7.69643
Memory consumed in KB	92	118	180	325	420	800	1067	1500	2258	2810

Smart Service based Response Analysis

Analysis is carried out based on the smart services such as Smart Agriculture, Smart Health and Smart Traffic. The analysis is made for 1000 requests for every smart service. Table 2. presents the factors bandwidth utilized, packet drops and success rate.

Table 2. Analysis based on Smart Services

Services	No. of requests	Packet Drops (%)	Bandwidth Utilized (Mbps)	Success Rate (%)
Smart Agriculture	1000	0.7	19.53125	99.3
Smart Health	1000	0.2	39.0625	99.8
Smart Traffic	1000	1.2	76.5625	98.8

Table 2. states that the packet drops for the service data transferred based on the request with regard to Smart Agriculture is less compared to the other two smart services. It is because of the lesser bandwidth utilized to carry the data relevant to the service requests to Smart Agriculture. Smart Traffic utilizes the bandwidth of 76.56 Mbps which is the highest of all the services. Smart Agriculture records high success rate of 99.3 %, whereas the Smart Health records 99.8% and the Smart Traffic records the lowest of 98.8% because of the various factors in the corresponding SSE.

8. Feasible Applications

The feasible and potential applications which could be incorporated in the proposed architecture for establishing IoT Information Kendra are listed below

- Smart Agriculture
- Smart Parking

- Smart Health Monitoring
- Smart Traffic Control
- Smart Crowd Control
- Smart Home
- Smart City
- Smart Metering
- Smart Emergency Alerts
- Smart Fire/ Gas Detection
- Smart Toilets
- Smart Transport / Logistics
- Smart Garbage Collection
- Smart Pollution Control
- Smart Library
- Smart Attendance

9. Social Contribution

As the leading IT industries across the globe are investing huge money in the field of IoT, there may be potential need for the proposed architecture to deploy many IoT enabled smart services by integrating them using IoT Information Kendra. Therefore a service provider may give variety of IoT enabled services to the users which benefit both the service provider as well as the user. The research out comes lead to apprehend its potential advantages for building sustainable and innovative smart cities. The Indian Government is envisioned to make many Indian cities into smart cities. The proposed architecture may be suitable for the Smart city projects. The Government may establish IoT_IK in District or Taluk level to host IoT enabled heterogeneous services to the general public. So, the proposed architecture will be of great use to the Government, IT industries and general public for availing and providing IoT smart services anywhere, any time. The life style of rural India will become more smarter by exposing people in villages to the IoT smart services and applications in their own day today activities.

10. Conclusion and Further Work to be done:

This minor research project has come out with the feasibility of integrating the different sectors under a smart services environment duly supported by IoT Information Kendra. The outcomes of the minor research project i.e, the architecture for integrating the IoT Smart Services will have its significant contribution towards scientific and social development. A revolution in

making human life smarter is possible with the help of this research outcomes with the other related technological advancements. The proposed IoT information Kendra will serve general public with many services if they are established in each district or region. This IoT Information Kendra will facilitate the registered users to avail any of its IoT enabled services and applications at anytime, anywhere and using any device across the globe. By integrating IoT enabled smart services and applications, millions of devices and objects connected to the environment, for sensing, inferring and interacting with each other to facilitate intangible benefits to the society at large. This research has brought out some feasible applications in each domain. The deployment of this proposed IoT based Smart Environment will be difficult but at the same time it has numerous benefits to the society in near future.

Each smart service will be extremely diverse and heterogeneous with regard to the communication technologies and resource capabilities may complicate the deployment of integrated IoT enabled services. As the IoT based smart environment has enormous benefits the number of challenges and issues are many and they have to be addressed properly. In particular, the security issues are to be addressed in future work.

References :

- [1.] [Yulongshen et. al., 2017] . Shen, T. Zhang, Y. Wang, H. Wang and X. Jiang, "MicroThings: A Generic IoT Architecture for Flexible Data Aggregation and Scalable Service Cooperation," in *IEEE Communications Magazine*, vol. 55, no. 9, pp. 86-93, doi: 10.1109/MCOM.2017.1700104, 2017.
- [2.] [Tao Zhong et. al., 2015] T. Zhong, K. A. Doshi, Z. Lu and G. Deng, "Capability Adaptive Elastic IoT Architecture," *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, pp. 615-622, doi: 10.1109/SmartCity.2015.138, 2015.
- [3.] [Dimitrious et. al., 2015] D. Georgakopoulos, P. P. Jayaraman, M. Zhang and R. Ranjan, "Discovery-Driven Service Oriented IoT Architecture," *2015 IEEE Conference on Collaboration and Internet Computing (CIC)*, Hangzhou, pp. 142-149, doi: 10.1109/CIC.2015.34, 2015.
- [4.] [Francois carrez et.al.,2017] F. Carrez, T. Elsaleh, D. Gómez, L. Sánchez, J. Lanza and P. Grace, "A Reference Architecture for federating IoT infrastructures supporting semantic interoperability," *2017 European Conference on Networks and Communications (EuCNC)*, Oulu, pp. 1-6, doi: 0.1109/EuCNC.2017.7980765, 2017.

- [5.] [Soumya kanti et. al., 2014] S. K. Datta, C. Bonnet and N. Nikaein, "An IoT gateway centric architecture to provide novel M2M services," *2014 IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, pp. 514-519, doi: 10.1109/WF-IoT.2014.6803221, 2014.
- [6.] [Souwmya et. al., 2016] S. K. Datta, C. Bonnet, R. P. Ferreira Da Costa and J. Härrí, "DataTweet: An architecture enabling data-centric IoT services," *2016 IEEE Region 10 Symposium (TENSYMP)*, Bali, pp. 343-348. doi: 10.1109/TENCONSpring.2016.7519430, 2014.
- [7.] [Yanuarics et. al., 2012], Y. T. Larosa, Jiann-Liang Chen, Yi-Wei Ma and Sy-Yen Kuo, "Socio-organism inspired model forming multi-level computational scheme for integrated IoT service architecture," *2012 2nd Baltic Congress on Future Internet Communications*, Vilnius, pp. 68-71, 2012.
- [8] Zhao Liqiang, Yin Shouyi, Liu Leibo, Zhang Zhen, Wei Shaojun, "A Crop Monitoring System Based on Wireless Sensor Network" *Procedia Environmental Sciences* 11 (2011), pp. 558 – 565.
- [9] M. Zhang, T. Yu, G.F. Zhai, "Smart Transport System Based on The Internet of Things", Amm. 48-49 (2011), pp. 1073-1076
- [10] Comton, M et al., "A Survey of the Semantic Specification of Sensor", proceedings of the 8th International Semantic Web Conference (ISWC 2009), 2 nd International Workshop on Semantic Sensor Networks.
- [11] QI Ai-qin, SHEN Yong-jun, "The Application of Internet of Things in Teaching Management System" International Conference of Information Technology, Computer Engineering and Management Sciences, 2011, pp. 239- 241.
- [12] Xu Li et al, "Smart Community: An Internet of Things Application", *IEEE Communications Magazine*, November 2011, pp. 68 – 75.
- [13] Martin Fiedler and Stefan Meissner, "IoT in Practice: Examples: IoT in Logistics and Health", *Enabling Things to Talk*, Springer, Chapter 4, pp. 27-36.

List of Papers Published:

- **A. Vimal Jerald**, Dr. S. Albert Rabara, A. Arun Gnana Raj "Secured Architecture for Integrated IoT Enabled Smart Services", *International Journal of Recent Technology and Engineering (IJRTE)*, Volume-8 Issue-3, September 2019, pp. 7384-7393, (ISBN: 2277-3878). (**Scopus Indexed Journal**)
- **A. Vimal Jerald**, and Dr. S. Albert Rabara, "End to End Secured Architecture for Internet of Things Information Kendra (IoT_IK) Integrating IoT Enabled Smart Services and Application", *International Conference on Mobile Computing and Sustainable Information (ICMCSI 2020)*, Organised by Thirubuvan University, Nepal, 23 January 2020. (Conference Proceedings will be published soon by **EAI/Springer ICC**) (**This research paper was selected as the best paper of the conference**)

CERTIFICATE



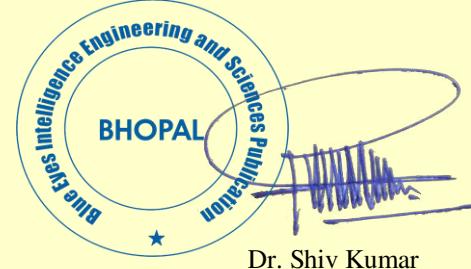
ELSEVIER
Scopus

This certifies that the research paper entitled '**Secured Architecture for Integrated IoT Enabled Smart Services**' authored by '**A. Vimal Jerald, S. Albert Rabara, A. Arun Gnana Raj**' was reviewed by experts in this research area and accepted by the board of 'Blue Eyes Intelligence Engineering and Sciences Publication' which has published in '**International Journal of Recent Technology and Engineering (IJRTE)**', ISSN: 2277-3878 (Online), Volume-8 Issue-3, September 2019. Page No.: 7384-7393.

The B Impact Factor of IJRTE is 5.92 for the year 2018. Your published paper and Souvenir are available at: <https://www.ijrte.org/download/volume-8-issue-3/>



Jitendra Kumar Sen
(Manager)



Dr. Shiv Kumar
(CEO)

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 (M₂M) 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

Revised Manuscript Received on September 25, 2019.

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.

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 in order 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 etc., 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]. 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 (T IoT). 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



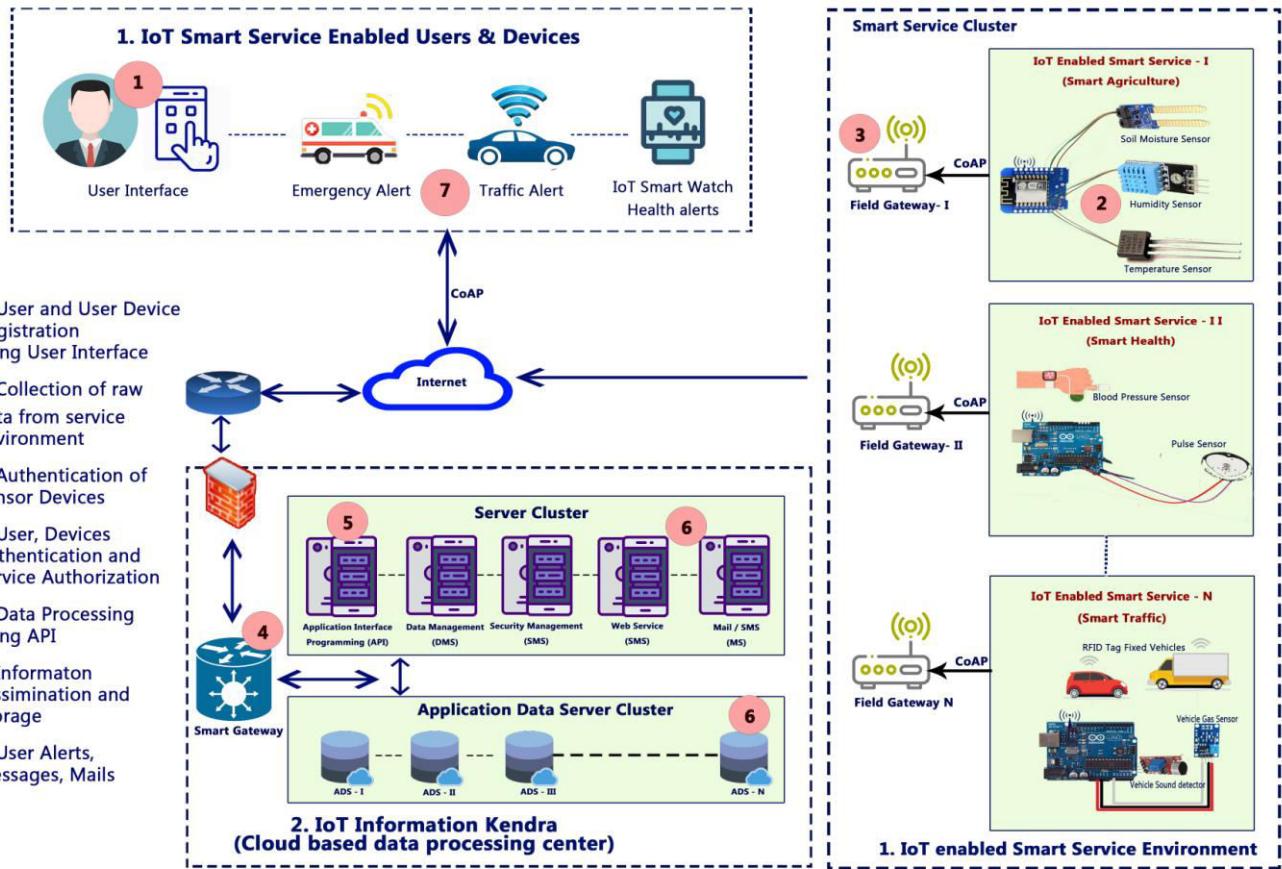


Figure 1. Architecture for Integrated Internet of Things (IoT) enabled Smart Services

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 etc. 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.

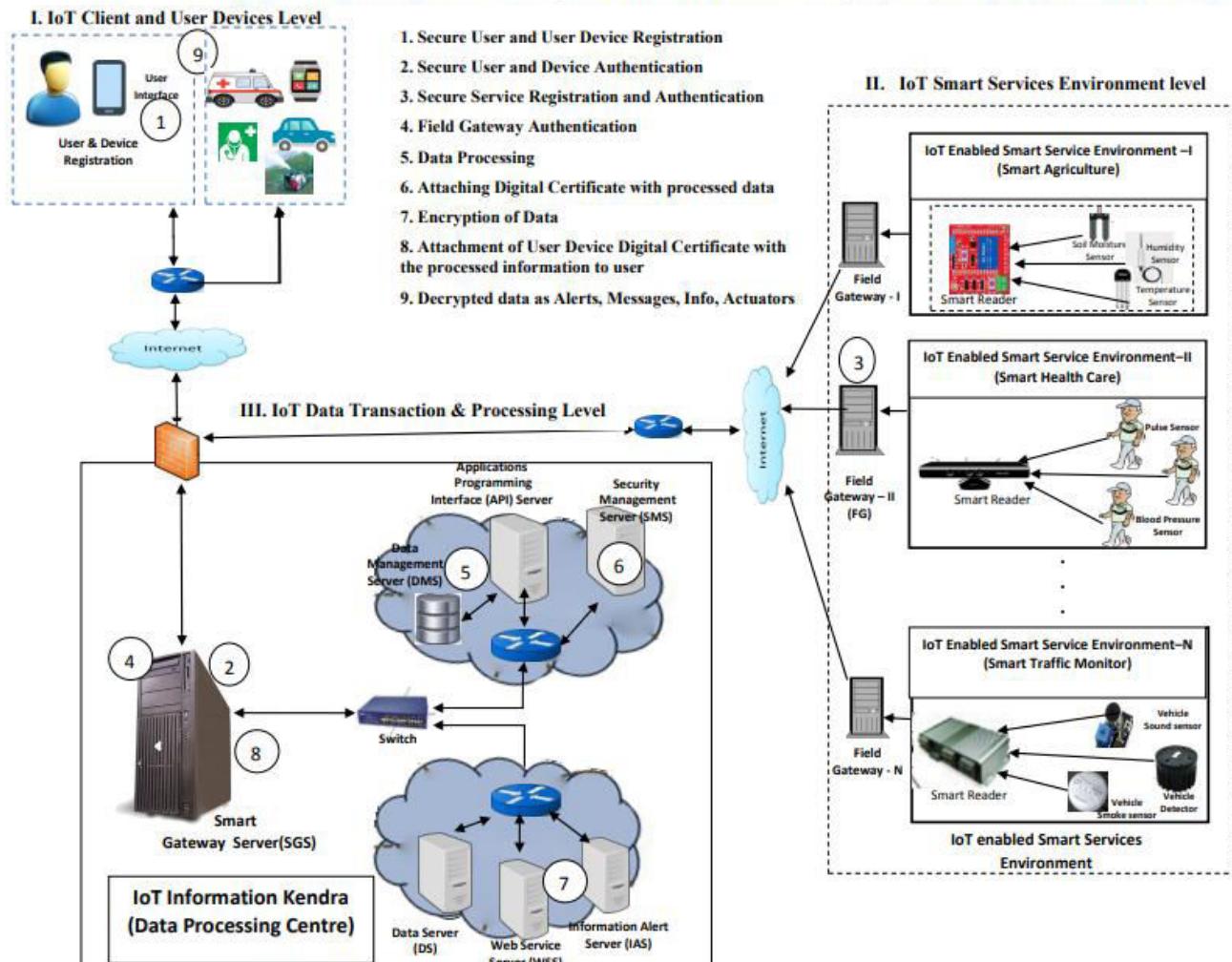
▪ Secure User and Device Registration

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



Secured Architecture for Integrated IoT Enabled Smart Services

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 $e2 = \text{Pairs.e1}$ where $e2 \in E_p(a,b)$ and computes the public key ‘ppk’ as $E_p(a,b), e1, e2$. 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 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 enabled smart services and avail information the user wants. If there is mismatch of the credentials the communication will

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 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 pairs 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 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 device 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 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 requester. The ping response time graph for ECC is presented in figure 9.

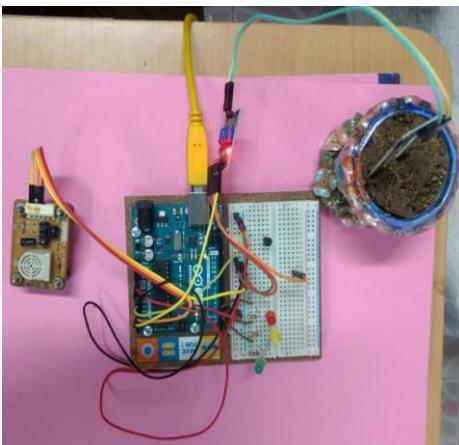


Figure 3. Arduino Generic Kit with Sensors

```
smart_Agri | Arduino 1.8.2
File Edit Sketch Tools Help
smart_Agri
void setup() {
  // put your setup code here, to run once:
  Serial.begin(9600);
  Serial.println("CLEARDATA");
  Serial.println("LABEL,Time,Temperature,Humidity,Soil");
}

void loop() {
  // put your main code here, to run repeatedly:
  Serial.print("DATA,TIME,");
  int sensorVal = analogRead(A0);
  //Convert reading to voltage
  float voltage = (sensorVal/1024.0) * 5.0;
  //convert millivolts into temperature
  float Temperature = (voltage - 0.5) * 100;
  float Humidity=((5.0*analogRead(A1)/1024)/0.033);
  int Soil = analogRead(A2);
  Serial.print(Temperature);
  Serial.print(",");
  Serial.print(Humidity);
  Serial.print(",");
  Serial.println(Soil);
  delay(10000);
}

Done uploading.
```

Figure 4. Arduino Development Kit 1.8.2attached

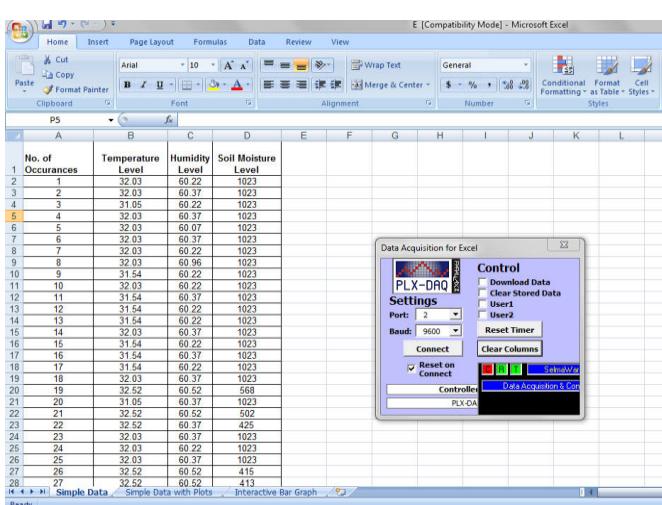


Figure 5. Record Set acquisitioned for Temperature, Humidity and Soil Moisture

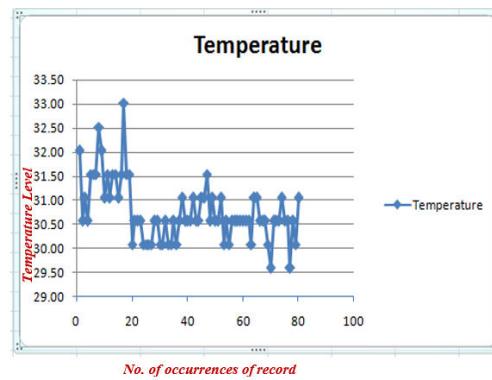


Figure 6. Temperature data recorded

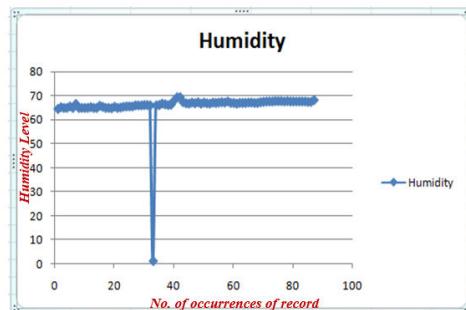


Figure 7. Humidity data recorded

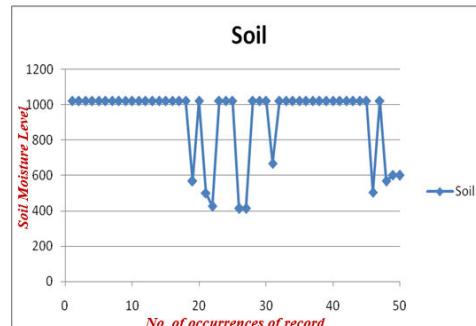


Figure 8. Soil Moisture data recorded

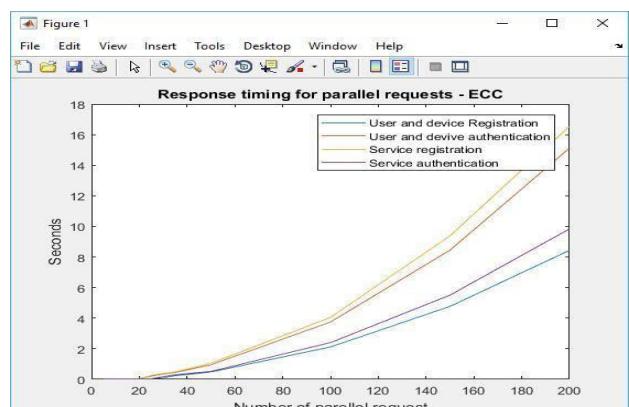


Figure 9. Ping Response time for the security functions 1.8.2attached

▪ 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**

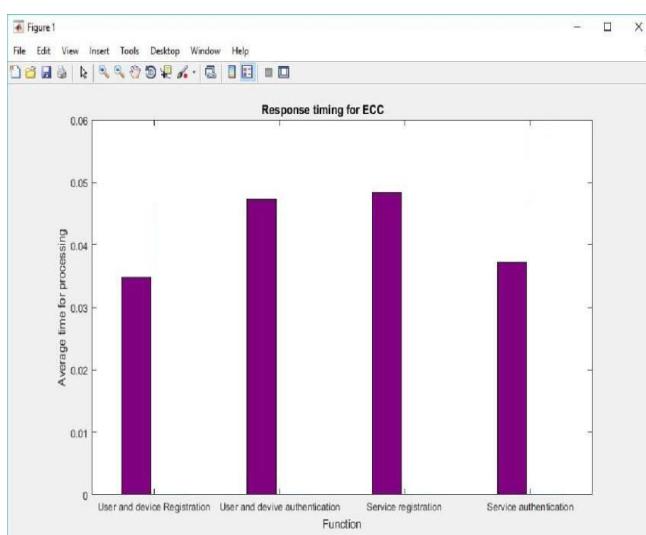


Figure 10. Response Time Processing

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.

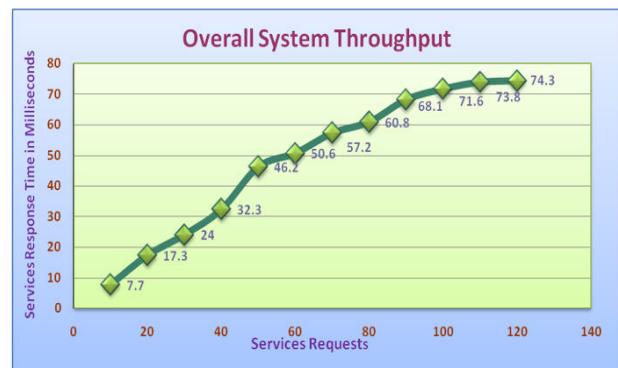


Figure 11: Overall System Throughput

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.



Secured Architecture for Integrated IoT Enabled Smart Services

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 et.al., 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.





CERTIFICATE OF PRESENTATION

This certificate is awarded to

A. Vinay Jaiswal

has successfully presented a paper entitled

End to End Secured Architecture for Internet of things

Information kendsn (IOT-IK) Integration IoT Enabled Smart Services Application

in the International Conference on Mobile Computing and Sustainable Informatics (ICMCSI 2020)

organised by Pulchowk Campus, Institute of Engineering, Tribhuvan University, Nepal

on 23-24 January 2020.

A handwritten signature in black ink.

SESSION CHAIR

A handwritten signature in black ink.

ORGANIZING SECRETARY

Dr. Jennifer S. Raj

A handwritten signature in black ink.

CONFERENCE CHAIR

Prof. Dr. Subarna Shakya



PROCEEDINGS
of the
**International Conference on Mobile Computing
and Sustainable Informatics**
(ICMCSI 2020)

23-24 January 2020

Technical Sponsors



End to End Secured Architecture for Internet of Things Information Kendra (IoT_IK) Integrating IoT Enabled Smart Services and Applications

A. Vimal Jerald¹, S. Albert Rabara¹
¹St.Joseph's College (Autonomous)
(affiliated to Bharathidasan University)
Tiruchirappalli - 620002
¹vimaljerald@gmail.com

Abstract. Internet of Things (IoT) is rapidly emerging paradigm connecting things such as objects and smart devices to deploy smart applications using heterogenous technologies. Security is the significant challenge in IoT. The security challenges are numerous when wide variety of IoT based smart applications integrated. This article proposes a end to end secured architecture for integrating IoT enabled smart applications and services through Internet of Things Information Kendra (IoT_IK). The proposed architecture ensures multilevel security using Elliptic Curve Cryptography.

Keywords: Internet of Things (IoT), IoT Information Kendra (IoT_IK), Elliptic Curve Cryptography, IoT Security Architecture.

1 Introduction

Internet of Things(IoT) is a convergence of devices, things and objects using sensor devices and related hardware for intelligent identification and tracing by data exchange using communication techniques[1]. IoT is so popular today because of some potential applications such as smart health, smart agriculture, smart traffic, crowd monitoring, smart city projects etc.,[2]. The existing IoT based applications and services are bound to single domain or a sector. The user needs to request different service providers geographically diverse to access these services. It is vital to integrate the various IoT based smart services and applications.

Security issues at large arise when millions of objects, devices and things communicate using wireless technology in an integrated environment for deploying various smart applications and services. Any leakage of information from any of the IoT devices/sensors could severely damage the privacy and

authenticity of the users and data. Even if the wireless technologies are secured by their own, their integration generates new security requirements. The creation of end-to-end secure channels could be one of the steps in the creation of security integration in IoT architecture [3]. Confidentiality and Integrity are few other major security concerns need to be addressed. Security solutions for IoT environment are entirely different from the conventional techniques as IoT is a network of tiny devices. So, energy efficient encryption and decryption techniques are to be used. It becomes essential to mitigate the security threats of IoT smart applications and services in an integrated environment. Proper remedies in an integrated perspective are devised envisaging a multilevel security architecture for integrated IoT based smart services and applications.

2 Related Work

Fugen Li et. al., have proposed a heterogeneous encrypting home works online / offline to establish secure data communications over sensor node of IoT and internet host. It is concluded that the proposed method provides solution for security issues when integrating WSNs into the Internet as part of the IoT[4]. Xuanzia Yao et. al., have put forth a scheme of lightweight multicast authentication mechanism for small scale IoT applications. Other security concerns like privacy, authorization and integrity are not addressed in the article[5]. R. Shadid et. al., have designed a light weight scheme for secure constrained application protocols (CoAP) by compressing the header of Datagram Transport Protocol Security (DTLS) messages. The different types of security attacks have not been addressed when constrained devices are connected by CoAP[6]. Sherin. P. et. al., have proposed a multilevel authentication system for smart home applications. The proposed system facilitates various security properties such as data confidentiality, integrity, forward security, privacy preservation and mutual authentication [7]. B. Vaidya et. al., have come out with a secure device authentication mechanism for smart energy home applications. This system does not provide enough information to prove that it is better than other authentication mechanism and how it is secure against attacks. Hence, it is essential to improve the authentication scheme which should satisfy the security factors like data confidentiality and integrity[8]. Xu Xiaohui has explored the various security mechanisms in Internet of Things such as safety certification and control technology supported with equipment authentication mechanisms[9]. Q.Wen et. al., have presented a technique for ID authentication at sensor nodes of IoT. It is a dynamic variable cipher which is deployed using a pre-shared metrics between the communication parties. In the work presented, the insulation of pre-shared metric needs to be secured for the work and it should be implemented for a large number of IoT devices. Only then the presented work can be applicable for the real time deployment of IoT based application where dynamic variable cipher security certificate is applied[10].

P.N. Mahalle et. al., have dealt with identity authentication and capability based Access Control (IACAC) for the Internet of Things. The authors have attempted to match integrated protocol with both authentication and access control capabilities to realize mutual identity implementation in IoT[11]. R. Mahmoud et. al., have explored the challenges in IoT security with the prospective measure. They have presented the security issues and mitigations to be taken in each layer of IoT. Confidentiality, integrity, availability and authentication are these security measures which must be lightweight and heterogeneous in nature[12]. Prem et. al., have proposed a novel technique for privacy preservation of IoT and introduced a preserving privacy in IoT architecture. The authors have implemented the proposed system which is proved to be an efficient system ensuring IoT data privacy. As like privacy the other security concerns like confidentiality authentication, integration are not addressed[13]. Don Chen et. al., have presented a secure architecture for Internet of Things to analyze the security challenge and threats[14]. Qi Jing et. al., have explored security problems of each layer of IoT architecture and have put forth solutions[15]. Quardeng et. al., have analyzed the security issues of the layers in IoT architecture such as perception layer, Network layer and Application layer. The authors have presented the construction of secure IoT and the secure strategies for fixing the security threats existing [16]. K. Jaswal et. al., have proposed a security securing Internet of Things. The article has listed various IoT protocol used, security challenges in IoT systems, Network layers of IoT architecture, and IoT security threats[17]. A White paper on security in Internet of Things by Wind River System has explored the security constraints in the IoT environment[18]. The literature has revealed that there are many IoT enabled applications and services work independently. There is no literature cited the integration of IoT smart services into architecture with end to end security.

Hence, a novel architecture integrating Internet of Things (IoT) enabled smart applications and applications is proposed in the paper. From the related work, it is clear that integrated IoT enabled smart services and applications to be secured by ensuring user authentication, device authentication, confidentiality, integrity and Data security. Many researchers have attempted to give adequate security using RSA which are bound to be with limitations such as lengthy key size, much time for computation and less energy efficiency. Daisy et. al., have dealt with a security framework based on Elliptic Curve Cryptography (ECC) for IoT services. It is proposed that ECC is applied in constrained devices with less memory storage. ECC is more efficient computationally than RSA and so, the security level achieved by RSA with 1024 bit key can be achieved with 160 bit key using ECC[19]. It is a security mechanism to address security concerns end to end while deploying or implementing of IoT Smart Services. The literature cited reveal that there is no integrated architecture exists to avail IoT enabled smart applications

and services. A unique and novel end to end secured architecture for Integrated IoT enabled Smart Services is proposed and tested.

3 Proposed Security Architecture

The proposed secured architecture integrating Internet of Things smart services and applications is designed with end-to-end strong multilevel security factors such as confidentiality, mutual authentication, integrity and privacy. The user authentication, device authentication process and service authentication process at SG of IoT_IK ensure the mutual authentication and other security factors with support of the security algorithms. The security support for proposed architecture is enhanced by adopting various security mechanisms by incorporating ECDSA based certificate, Elliptic Curve Cryptosystems.

The three different level security are adopted with multilevel authentication using ECC. The security architecture proposed with the various security processes are depicted in Figure 1. The proposed security architecture which ensures stronger security for the integrated IoT smart applications and services. The security processes at levels at the proposed architecture such as secure user registration and device registration, secure user authentication and device authentication, secure service registration and secure service authorization which are subsequently explained in detail.

3.1 Major Components

The proposed Architecture comprises of three units such as IoT Smart Services Environment (IoT SSE), IoT Information Kendra(IoT_IK) and IoT Client. IoT Smart Services Environment consists of Sensor Devices (SD), Smart Readers (SR) and Field Gateway (FG) are connected appropriately in IoT SSE. IoT information Kendra(IoT_IK) is designed for data aggregation and data analysis appropriately with respective applications. IoT_IK comprises of Server Cluster (SC), Application Data Server Cluster (ADS), and Smart Gateway (SG). The Service Cluster (SC) in IoT_IK comprises of different servers such as Application Programming Interface Server (APIS), Security Management Server(SMS), Application Data Server (ADS), Data Management Server (DMS), Web Services Server (WSS) and Information Alert Server (IAS). IoT Clients are mobile devices, IoT embebeded alarms, Emergency alerts system, Smart Watches, IoT connected vehicles, actuators etc.,

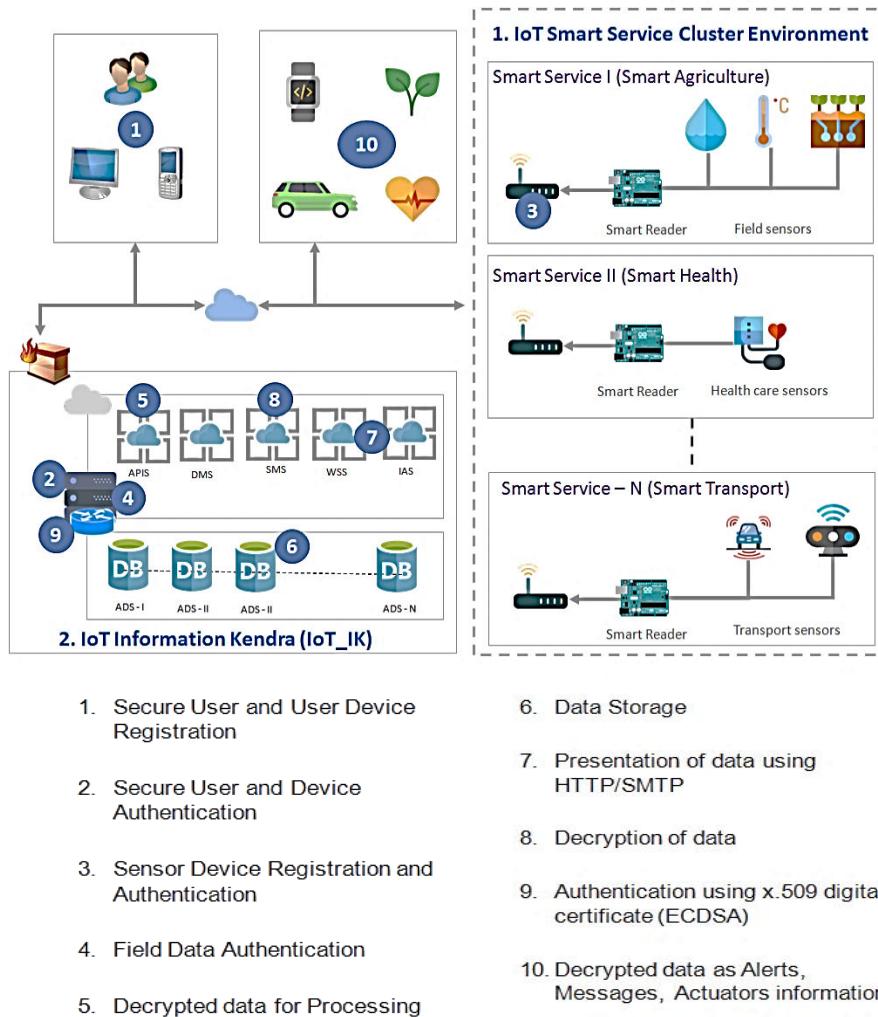


Fig. 1. Proposed End to End Security Architecture

3.2 Functionality of the security architecture

The proposed architecture enables the integration of IoT smart applications and smart services which facilitate the user to access the IoT services securely anytime, anywhere and with registered device. The user establishes a connection with Smart Gateway(SG) at Internet of Things Information Kendra (IoT_IK) using Hyper Text Transfer Protocol (HTTP) via internet. The user with the help of User In-

terface (UI) at the user's device requests the SG for the secure user authentication and user device registration. The user through UI feeds the user details such as name, DoB or age, aadhaar number, mobile number and email id. The user device credentials such as MAC id or IMEI and IP address are extracted automatically. User is primarily authenticated using OAuth at SG by sending a One Time Pin (OTP) to the mobile number entered by the user for the primary verification. On successful verification of mobile number, User id (U_id) and Device id (D_id) are generated by the SG using user and Device credentials. Certificate registry at SG generates the user certificate based on ECDSA by encrypting U_id and D_id using ECC. Key pairs such as Public Key (PuK) and Private Key (PtK) are also generated using ECC cryptosystem. The generated user certificate is stored in certificate registry at SG along with PuK. The same user certificate is sent to the user device along with PtK for further authentication.

The sensor devices, objects and Smart Readers (SR) at at Smart Service Environment (SSE) are registered with corresponding Field Gateway (FG) of SSE. The inferred raw data by the sensor devices are read by Smart Reader (SR) and the same is sent further to the FG. A network communication is established between FG and SG of IoT_IK using Constrained Application Protocol (CoAP). FG using the UI, requests SG for service registration. The service credentials such as service name, service type, IoT Devices id allocated by FG, MAC id and IP address of FG are used to generate S_id and IoTD_id after fundamental authentication using Oauth at SG. Certificate registry at SG generates a service certificate using S_id and IoTD_id along with PuK and PtK generated using ECC. The service certificate generated is stored in the certificate registry along with its PuK. The same certificate is sent to FG along with PtK.

The raw sensed data from SSE are sent by FG along with the corresponding service certificate is sent to SG using CoAP over the established connection between FG and SG. The service is authenticated securely at SG using credentials in service certificate with the stored credentials at certificate registry. The PuK at SG and PtK are sent by FG are used to decrypt the data in the certificate. On successful authentication, the sensed data are sent by FG are further sent to Application Programming Interface Server (APIS) for data analysis. The sensed data is received at APIS at a fixed time interval after the secure authentication of services. APIS aggregates and processes the data based on the service using the respective algorithms. Data Management Server (DMS) supports the APIS with the GPS information and other information related the SSE. Web Service Server (WSS) helps the APIS with web based services on demand to supplement data processing. The processed data are stored at Application Data Server (ADS) regularly. If the processed data reaches a threshold state based on the algorithm, the data is to be sent to the IoT client as alerts or messages. Information Alerts Server (IAS) facilitates APIS for message formatting based on the IoT client. The Security Management

Server helps encrypting the alert information with the help of ECC cryptosystem. The encrypted form of alerts and messages to IoT client are sent with PuK from SG. The PuK is sent along with the message or alert and the PtK with the user or IoT client will decrypt the data. Hence, only the appropriate user or IoT client will receive the alerts or messages securely.

When the user requests SG at IoT_IK for a service using UI at the user's device, the service certificate is sent along with the PtK, SG will validate the credentials in the certificate decrypted by respective PuK. The secure user and device authentication is carried by matching the credentials of the certificate and the credentials stored at certificate registry. On successful authentication, the user request is further sent to APIS for the requested data. APIS in turn processes the request and with the help of other servers of Service Cluster (SC) at IoT_IK. SG establishes a secure communication between IoT_IK and IoT client or the user device using HTTP. The requested service information is sent to the user or to the IoT client through SG. The service information in an encrypted form with PuK is sent to the user devices. The user device with the help of PtK decrypts the data. So, it is possible only for the appropriate user device to receive the requested service information securely. Figure 2 illustrates the functional components of the proposed secured architecture.

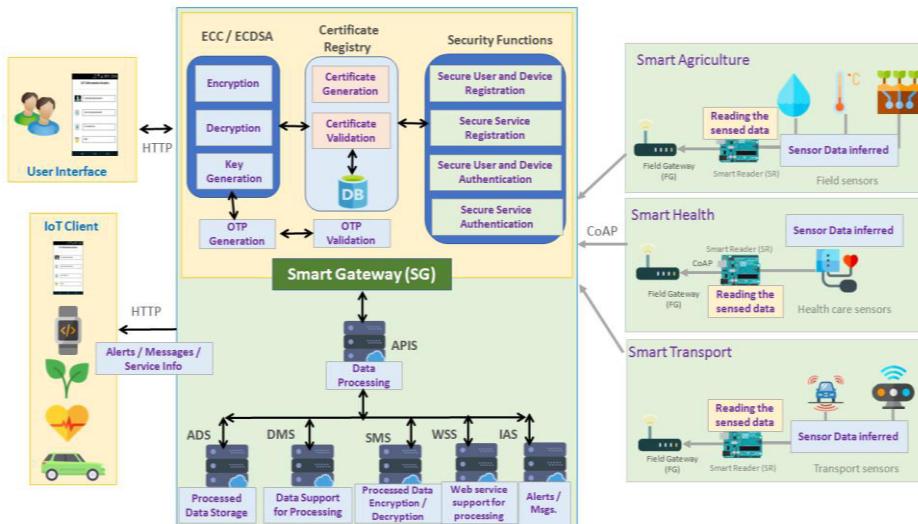


Fig. 2. Functional Components of the Proposed Architecture

3.3 Multilevel security at the proposed architecture

The research proposes a stronger security for the proposed architecture in different levels such as Client, IoT Smart Services Environment(IoT_SSE) and IoT Data Transaction and Processing.

3.3.1. a. IoT Client and Device Level

The registered IoT Client and IoT devices used are authenticated and authorized at the Client level security with the help of ECDSA certificate and message exchange using ECC. All the data transferred from the SSE Level to the Client level through the IoT_IK are encrypted and decrypted with ECC. Digital certificates are also used to authenticate registered IoT devices to ensure integrity and confidentiality of the information. User authentication is carried out to assure users' privacy. Only the registered user may avail the authorized service using the registered device. So, there is no possibility of unauthorized access of service and it is not feasible for the unauthorized service to communicate the user.

3.3.2. IoT Smart Services Environment Level

All the smart devices and sensors connected in a SSE are to be registered and authenticated in the FG by obtaining their IoTD_id (Device id), and MAC ID. The FG receives the information from the IoT devices and encrypt the information and establishes a secure communication using CoAP with the SG of IoT_IK using digital certificate. The SG verifies the credentials in digital certificate generated during the registration process and receives the encrypted data for further analysis. This phase ensures that only the registered IoT devices may send raw data and through which confidentiality is achieved. It is not feasible for the intruders to access the IoT devices as like FG.

3.3.3. Internet of Things Information Kendra Level

The Smart Gateway establishes secure communication using **HTTP** with the **APIS** using mutual authentication and forwards the encrypted data to **APIS** for data aggregation and analysis of information. The **APIS** decrypts the information and processes the data based on the algorithms according to the services and applications. The **APIS** then establishes a communication with **IAS** through the **SMS** for sending messages or alerts to the registered users and the smart devices. Service authentication process assures integrity and thus there is no chance of authorized service providers to influence the actual data inferred from **SSE**. The messages or alerts are sent to the appropriate user who requested the service, based on the user credentials in the certificate attached.

3.4. Secure Data Communication between FG and SG

The proposed architecture lays a secure connection between the FG and SG after successful authentication using the X.509 digital certificate via Secure Socket Layer (SSL) protocol. CoAP Protocol is responsible for the secure data communication between FG and SG. FG requests a connection with SG by sending PtK and ECDSA service certificate X.509. SG checks the authenticity of the certificate using the corresponding PuK and other stored credentials of FG. If the authentication is successful, the FG can be trusted and further data transaction is permitted. The session keys are exchanged securely between the SG and FG. The sensor data from the IoT SSE can be securely transmitted over the established channel. The raw data or the inferred information from SSE via FG are taken to Application Programming Interface Server (APIS) of IoT_IK for data aggregation via SG. The data transaction between FG and SG take place securely by service authentication i.e., by verifying the credentials stored in the certificate of the respective service. If the credentials in the certificate and the credentials of service fetching raw data from the FG match the data fetched from service environment, is taken to APIS securely

3.5. Architecture level Secure Data Processing

The user registered with a registered smart mobile device using the UI requests for any service to SG at IoT_IK. The request from the user is sent using HTTP along with the user and device certificate which consists of the user and device credentials. User and device certificate authentication at SG based on OAuth authentication method is carried out with the credentials extracted from certificate registry. If the credentials extracted from service registry and the credentials with certificate match, the user and device are authenticated successfully. On successful authentication, user request is further sent from SG to APIS for the necessary action rather process. Similarly the raw data from SSE are sent through FG to SG at IoT_IK for data aggregation. The raw data is attached with the service certificate which comprises of service credentials and credentials of SG along with PtK. The CoAP protocol is used for data communication between SSE, FG and SG. If the credentials with the service certificate, PtK and the credentials extracted from certificate registry for the corresponding SSE match, the service is then authenticated. On successful authentication, the raw data fetched from SSE is forwarded to APIS by SG for further action. The communication channel from SSE to SG through FG and the communication channel from the user to SG are secured using the proper security mechanism proposed in the architecture. The process of secure data communication at the architecture is depicted in Figure 3.

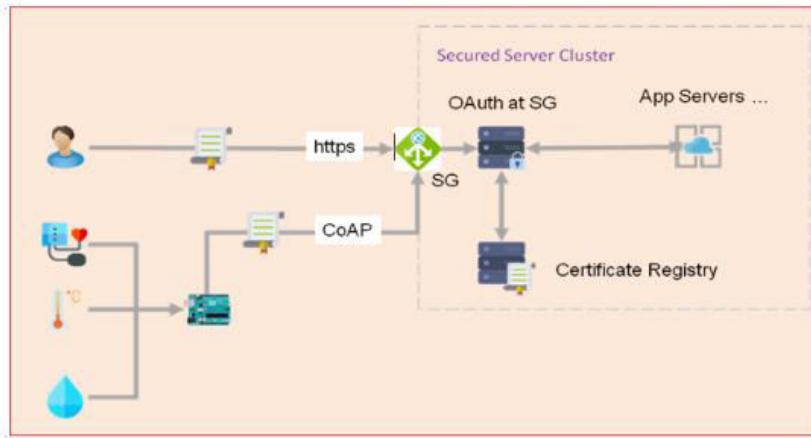


Fig. 3. Secure Data communication at Architecture level

4 Experimental Study

A Test Bed has been designed using an experimental setup for the proposed work. Secure user registration, device registration, secure service registration, secure user and device authentication and secure service authentication are performed to ensure the end to end security of the proposed architecture. The performance analysis on Ping Response Time, System Throughput and latency analysis guarantee that the proposed architecture functions efficiently with the enhanced performance.

4.1 Performance Analysis of Security functions

Ping response time for the proposed architecture using **ECC** cryptosystem and Self signed **ECDSA** certificate is generated over **SSL** with regard to each security functions such as User Registration, Device Registration, Service Registration, User and Device Authentication and Service Authentication with the inferred data set for the simultaneous requests ranges from 20 to 200 were tested with the increase of 20 requests. Response time for various security functions for parallel requests are tabulated in Table 1. and the response time taken for the security functions are graphically represented in Figure 4.

4.2. Analysis on Overall System Throughput

Performance analysis is done to compute overall System Throughput which is the total work done by the proposed system at given time. Table 2 presents the obtained overall system throughput for the system model based on the proposed ar-

chitecture. An analysis is made of system throughput for 1000 to 10000 parallel service accesses with the increase of 1000 requests. Time taken and bandwidth utilized are presented in the table. According to the obtained results given in the table, the time taken increase gradually when the service requests or access increases. It takes **261.600 seconds** for 10000 service accesses /requests to complete all the operations of the proposed architecture. Band width utilized for the service accesses or requests proportionately increase. It takes **29 Mbps** for 1000 service accesses on an average. It is proved from the results given in the table that the failed requests are very minimum i.e., it is only **0.15%** on an average for every 1000 service requests. Figure. 5. Illustrates the overall system throughput for the proposed system based on the architecture.

Table 1. Response Time for various security functions for the parallel requests

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

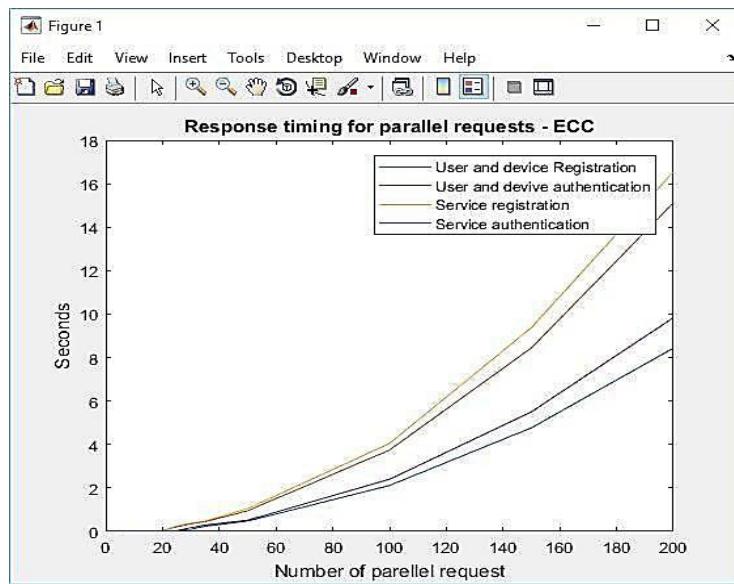


Fig. 4. Response time taken for Parallel requests

Table 2. Overall System Throughput

No. of parallel requests	Time Taken in seconds	Bandwidth Utilized (Mbps)	Failed Requests (%)
1000	2.943	29.30	0.20
2000	11.005	58.59	0.15
3000	25.645	87.89	0.13
4000	42.245	117.19	0.15
5000	68.426	146.48	0.14
6000	98.130	175.78	0.18
7000	128.582	205.08	0.17
8000	173.254	234.38	0.16
9000	215.623	263.67	0.19
10000	261.600	292.97	0.20

The overall performance of the proposed architecture proves to be efficient and secured based on the different performance tests conducted. Performance analysis results of various security functions ensure the secure communication between user and the **IoT_IK**. Similarly the data communication between **FG** at **SSE** and **SG** of **IoT_IK** and the communication between **SG** and IoT client take place securely. The time taken for various security processes and the time taken for accomplishing the service requests are very less. The failure rate rather failed service requests are very minimal.

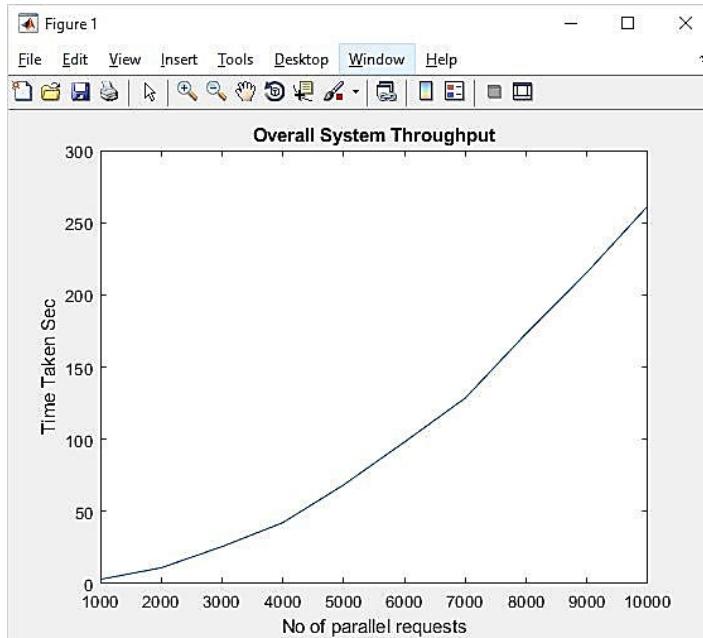


Fig. 5. Overall System throughput

5. Conclusion

Secured architecture integrating Internet of Things (IoT) enabled smart services is proposed to actualize the vision of availing IoT based smart services and applications by integrating heterogeneous devices and objects in diverse environment anytime, anywhere and in any device in a secured manner. This proposed architecture is adaptable and unique for the users to have secure access over diversified IoT smart applications and smart services. The proposed novel IoT Information Kendra (IoT_IK) will certainly help the government to provide smart services may benefit a billion of general public particularly people live in rural areas if it is established in every mandal or divisions. The proposed system will be a means of achieving Digital India mission of the Union government of India.

References

1. Elkhodr, The Internet of Things: Vision & Challenges, TENCON Spring Conference, IEEE, pp.218-222 (2013)
2. Dieter Uckelmann, An Architectural Approach Towards the Future Internet of Things, Architecting Internet of Things - Springer, pp. 1-22 (2011)
3. Debasis Bandyopadhyay, Jaydip Sen, "Internet of Things: Applications and Challenges in Technology and Standardization", Springer, Wireless Press Communication, pp. 49-

- 69, (2011)
4. F. Li and P. Xiong, "Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things," in *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3677-3684, (2013)
 5. Xuanxia Yao, X. Han, X. Du and X. Zhou, "A Lightweight Multicast Authentication Mechanism for Small Scale IoT Applications," in *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3693-3701, (2013)
 6. R. Shadid, H. Shafagh, K. Hewage, R. Hummen and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," in *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3711-3720, (2013)
 7. Sherin. P., S. Peter and R. K. Gopal, "Multi-level authentication system for smart home-security analysis and implementation," *2016 International Conference on Inventive Computation Technologies (ICICT)*, pp. 1-7 (2016)
 8. B. Vaidya, D. Makrakis and H. T. Mouftah, "Device authentication mechanism for Smart Energy Home Area Networks," *2011 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, pp. 787-788 (2011)
 9. X. Xiaohui, "Research on Safety Certification and Control Technology in Internet of Things," *2012 Fourth International Conference on Computational and Information Sciences*, Chongqing, pp. 518-521 (2012)
 10. Q. Wen, X. Dong and R. Zhang, "Application of dynamic variable cipher security certificate in Internet of Things," *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, Hangzhou, pp. 1062-1066 (2012)
 11. Parikshit N Mahale, Bayu A, Neeli RP, Ramjee P, "Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things", *Journal of Cyber Security and Mobility*, Vol. 1, pp. 309–348, (2012)
 12. 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, [2016]
 13. Prem Prakash Jayaraman, Xuechao Yang, Ali Y, Dimiritous G, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation" *Future Generation Computer Systems*, Elsevier, pp. 1-10, (2017)
 14. [Don Chen et. al.] D. Chen, G. Chang, L. Jin, X. Ren, J. Li and F. Li, "A Novel Secure Architecture for the Internet of Things," *2011 Fifth International Conference on Genetic and Evolutionary Computing*, Xiamen, pp. 311-314 (2011)
 15. Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, "Security of the Internet of Things: perspectives and challenges", Springer Science, pp. 2481-2500 (2014)
 16. Q. Gou, L. Yan, Y. Liu and Y. Li, "Construction and Strategies in IoT Security System," *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, Beijing, pp. 1129-1132 (2013)
 17. Komal Jaswal, Tampriya Choudury, Roshan Lal Chhokar, Sooraj R Singh, "Securing the Internet of Things : A Proposed Framework", *International Conference on Computing Communication and Automation (ICCCA2017)*, IEEE, pp. 1277-1281, (2017)
 18. Wind River System, "Security in the Internet of Things", White paper by Wind River System, pp. 1- 6, (2015).
 19. 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)