IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Major Domains of Internet of Things (IOTS) Based Applications and Associated Challenges

Dharmendra Patel[1*], Pranav Vyas[2], Atul Patel[3]

[1,2,3]Smt.Chandaben Mohanbhai Patel Institute of Computer Applications, CHARUSAT, Changa, Gujarat, India

DOI: https://doi.org/10.26438/ijcse/v7i6.810818 | Available online at: www.ijcseonline.org

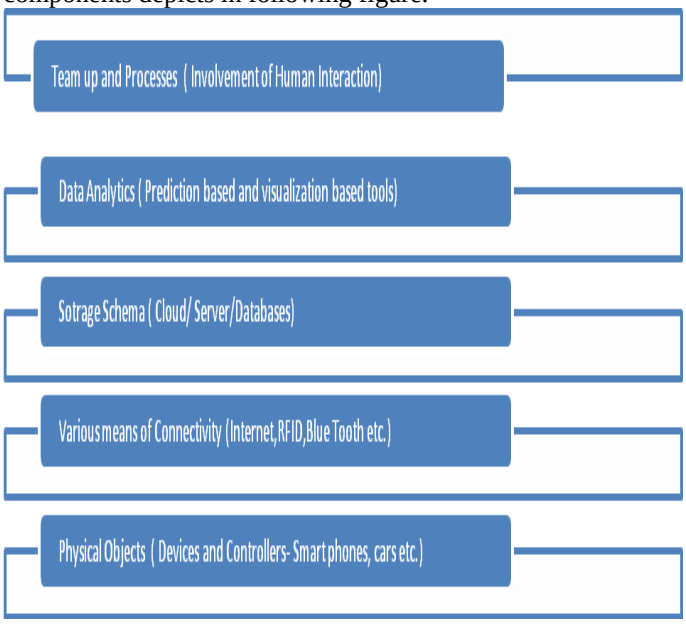
Accepted: 09/Jun/2019, Published: 30/Jun/2019

Abstract: In recent years Internet of Things (IoTs) concept has expanded in massive impetus due to very good Internet infrastructure everywhere. IoT has the ability to creating a network of physical things that use embedded technologies in order to sense, converse, cooperate, and team up with other things. IoT sets up sophisticated connectivity among physical things in order to make automation in specific areas. Several applications have been developed in all domains, based on IoT concepts, to collaborate with other physical things in order to achieve atomization in that area. This paper will focus on major applications of Internet of Things (IoTs) on various application domains. Internet of Things (IoTs) process is very complex in order to team up with other physical objects and deals with many challenges. This paper will also discuss with challenges of IoTs in various application domains.

Keywords: Internet of Things (IoTs), Embedded Technologies, Data Analytics, Controllers, Connectivity

I. INTRODUCTION

Internet of Things (IoTs) enables machine to machine communication by embedding physical objects with software, electronic circuitry, sensors and several means of connectivity. Internet of Things acts a system where different components act together in order to accomplish a specific goal. Internet of Things (IoTs) system has different components depicts in following figure.



(Figure 1. Components of IoT System)

Internet of Things(IoTs) based application is possible when all above mentioned components such as physical objects, connectivity, storage are interact with each other and based on that appropriate analytics and human interaction should be possible.

Efficient and successful implementation of IoT based physical objects may transform many aspects of human life. IoT based technology is useful in all domains of applications. Major IoT based applications domains are home automations, eHealth, retail, animal farming, industrial control, logistics, securities, water, environment, cities etc. We will discuss the applications of all domains at later stage. To develop IoT based applications, basically three steps are need:

1. Sensors, Electronic Circuitry or other technology required to connect to the device ranging from any physical object.
2. Send or receive data from network relating to characteristics of physical object.
3. Control the situation with controller if it is not behaving in proper manner.

To start any Internet of Things based application, one should think about four main phases. First phase is think about the thing itself. The thing contains all aspects in very small box such as low power processor, embedded operating systems and one or more communication protocols to communicate with external environment. The next phase is software and technical infrastructure that runs on server or any cloud

system that receives and managing data coming from the thing. The next phase is analytics that process data based on certain prediction based and visualization based tools. Final phase is human interaction with physical thing. To make any application effectively, analytics and human interaction phases should be given more attention.

Internet of Things based applications should follow certain characteristics.

- **Ambient Intelligence**: It is a responsive and sensitive to the presence of people. Ambient Intelligence allows people to carry out their routine activities through support of physical devices. IoT applications should contain more complicated forms of intelligence to work in real environment.
- **Event Driven Architecture:** It is a message driven architecture that reacts based on certain event. This kind of architectural pattern is useful in implementation of application which transmits events among components that are loosely in nature. In IoT applications, generally interaction among components are loosely and different components are unaware about other components.
- **Scalability:** Internet of Things applications requires scalability in terms of network to handle flow of various physical devices. Internet protocol version 6 (IPv6) is a vital to handle the network scalability.
- **Complex Interactions:** Internet of Things based physical objects require different links and complex interactions with different actors and should have a capability to integrate new one.
- **Size and Space**: Internet objects are trillion in number and IoTs requires precise geographic locations of a thing so size and space is one of the most important characteristics of IoTs.

The section-2 will deal with related work in IoT based applications. The section-3 will narrate different applications domains of IoTs with several applications. The section-4 will derive the challenges of IoTs. Finally paper ends with conclusion.

II. RELATED WORK

Internet of Things is a global network that consists of several diversified networks linked with wireless, optical and electronics based technologies [3] . Internet of Things concept is very vital for large corporations that have an ability to transform real word objects into intelligent virtual objects for the benefit of the masses [11]. From perspectives of the corporations; consequences of IoTs is visible in field of automation, manufacturing, logistics, business process management, transportations etc.[12]. There are various research have been done in this area based on different perspective such as architecture, security aspects and applications. Following table describes related work of Internet of Things based on different perspectives.

(**Table 1. Related work of IoTs based on different perspectives)**

Perspective	Reference Number	Description
Architectural Elements	[7]	Three architectural components are described in this paper such as Hardware, Middleware and Presentation. Authors discussed RFID, WSN-hardware, communication stack and middleware, data storage and analytics and addressing schemes related to different architectural elements.
	[25]	This thesis proposed a mobile wide area deployable WSN communication architecture. It is to be applied for food-IoT and health-IoT solutions. Author proposed a novel acceleration data compression algorithm for WSN with improved performance in compression ratio, complexity and scalability.
	[4]	In this paper authors favored an architectural approach that is based on extension of EPC global network. EPC global network is standardized architecture that is widely accepted by many industries.
	[1]	In this paper, integrated architecture for interconnecting WSNs and actuators is presented. Lightweight protocols 6LoWPN are used to achieve this. This architecture was validated by the guidelines of the largest European Project

		(SENSEI) on WSNs.
	[22]	In this paper author has described the application and development of the teaching platform architecture based on IoT. Architecture of teaching environment is designed based on perception equipment, access, unit, access network, middleware and application.
	[15]	The paper described Internet business environment architecture based on Web. Total four layers based on different user perspectives were indentified.
	[14]	In this paper Cognitive architecture based on IoTs was discussed. Cognitive and cooperative mechanisms which were integrated to promote performance and achieve intelligence.
Security	[16] [20]	In theses papers authors has focused on approach to Classifying threats. They have described most widely used ontology of security threats based on classic CIA and CIA+ models.
	[2] [17] [18]	Authors described integrity and hardware device based security based on attestation. Attestation ensures that firmware is unmodified and therefore the device is accurate.
	[19]	Authors have described some common threats on IoTs. Total eight kinds of threats are described by them.
	[9]	Authors have narrated RFID based security measures.
	[10	In this paper development trend of IPv6 based information security products was discussed in detail.
Applications	[5]	In this paper several applications, based on IoTs , were described by authors on various domains such as cities,environment,health, business etc.
	[13]	Authors attempted to categorize the service, provided by IoTs in order to help in designing efficient application development.
	[21]	This paper demonstrated how IoT transforming healthcare industry. It has proposed few applications of IoT in rural healthcare and ways to improve primary health needs of developing countries.
	[6]	It dealt with traffic problem based on integration of IoTs and agent technology. The architecture of an application introduced RFID, wireless sensor technology, ad hoc networking and internet based information system in which tagged traffic objects automatically represented, tracked and queried over network.
Applications	[8]	In this article authors designed IoT based smart crime detection system. The system was able to detect crimes in real time in South Korea by analyzing human emotions. Authors have described emotion sensing, emotion recording, crime detection, crime visualization and crime prediction modules.

	[23]	Authors have described security of food supply chain with help of IoT. Authors have presented traceability model of food supply chain that consists of sensing, communication and application layer.
	[24]	This paper presented intelligent car parking system based on cloud and IoT. In this, authors have provided many software solutions in order to get best car parking experience to mobile users.

In this paper we have focused more on applications as they involve both appropriate architecture and security aspects. In the next section major domains of IoT based applications will be discussed.

III. MAJOR DOMAINS OF INETERNET OF THINGS APPLICATIONS

"The fourth industrial revolution" initiated by Germany in 2011 is really become reality due to Internet of Things (IoTs) based applications. At the core of IoTs are millions of devices that transmit data and perform actions based on Internet connectivity. Every domain has number of possibilities to implement such kind of IoT based applications. Following table describes the major emerging domains and their IoT based applications with characteristics.

(Table 2. Emerging Domains of Internet of Things based applications)

Emerging Domain	IoT based Applications	Major Characteristics
Smart Cities	• Smart Roads • Smart Parking • Traffic Congestions • Waste Management • Smart Lighting	• Connecting people and data based on physical things to improve "livability"of communities • Utilizing ICT and Internet to address urban problems
		• Better monitoring by using intelligent sensors • High amount of Information Technology amalgamation and broad application of information based resources
Smart Agriculture	• Controlling of climate conditions • Improvement in yield • Recommendations • Reduce water requirement • Forecasting	• Overcome growing water scarcity, inadequate availability of lands, hard to deal with costs etc. • Data generated from GPS and sensors on the field and farming equipment • Analytics on data of soil, weather, water, crop prediction etc. • Provide new insights and recommendations to aid in better decision-making
Health care	• Patients observation • Fall Detection of disable people • Control of conditions of vaccines and medicines in freezer	• Distribute more precious data, reduce the requirement for direct patient-physician

	• Measurement of UV Radiation • Smart beds	contact • Health devices and sensors can be connected among each other and to a central gateway through various protocols • Devices are automatically configured according to the treatment plan and will be remotely checked by a doctor
Wearable Devices	• Smart Glass • Smart Watch • Activity Tracker • Mail Notification	• Helps users in multitasking and improve ways of life • Wearable device base IoT solutions can be deployed in various segments • Requires technical expertise in design, firmware development, programming language and ubiquitous computing
Retail Industry	• Smart shopping applications • Automate Restocking • Control supply chain • Location or activity based Payment • Digital Price tags	• Increasing store efficiency and customer experience • Connects people, products, devices and service to modernize the flow of an information • Speed up supply chain and security
Education	• Interactive Environment • E-Learning	• Learning is not confined to class room • Creates interactive and collaborative
Education	• Report System • Collaboration	Environment for teaching-learning • Easier for teacher to manage and organize lesson plan
Military	• Real time Decision Making • Soldier Healthcare • Cost reduction through asset tracking • Military Logistics	• Commanders benefits from sensor and camera based information mounted on ground and air vehicles • Generates and analyze more information • Improves communication and routing of an information.
Environment	• Control air pollution • Determine patterns of land conditions • Fire detection in forest • Detection of Water Quality • Determine Soil Condition	• Uses sensors for environment protection • Used by emergency services for betterment of an environment • Spans large geographic

		area than other domain applications
Manufacturing	• Automate Production Process • Reduction of maintenance cost • Controlling from remote • Analyzing data of processing	• Industries are more efficient, productive and smarter • Provide broad picture of entire manufacturing process • Improve asset utilization and optimization
Smart Home	• Controlling Energy use • Remote control appliances • Intrusion Detection • Video Monitoring	• Wi-Fi becomes more common in home networking • Allows user to control appliances of home remotely • User can investigate the circumstances of various home parameters

CHALLENGES IN INTERNET OF THINGS

Internet of things is a relatively new topic in discipline of computer science. There have been great deal of research in the field but most of the research concentrates on applications of IOT and its architecture. In our survey we would also like to draw attention of fellow researchers in challenges in rapidly changing and expanding discipline of IOT. The challenges in this discipline can be divided into following different categories: 1) Global Challenges 2) Business Model of IOT and New Currencies 3) Ethics, Control Society, Surveillance, Consent and Data Driven Life 4) Technological Challenges. Here in this paper we are concentrating on challenges of technical nature

We have identified four challenges that IOT faces today. 1) Data Security & Privacy 2) Data Sharing & Inter Operability 3) Hardware & Software Issues.

1. Data Security and Privacy Issues

Data Security can prove challenging due to number of reasons in IOT. An IOT network is made by large number of nodes that can communicate with each other and exchange data.

The first problem with data security of IOT devices is that almost all the devices uses wireless medium to communicate with other devices. This makes them susceptible to eavesdropping.

A limitation of IOT devices also lies in its size and processing capacity. Most devices are small. Due to its limited processing power it is difficult to implement the standard data security techniques on the device itself. This renders them open to attack from eavesdropping.

Another issue is since these devices are placed to passively monitor, it is easy to access them physically. This can result in data loss if user is able to access and separate the data storage module from rest of device.

These nodes are also equipped with sensors that can be used to capture various types of data. These types van vary greatly based on functionality of an IOT device for example, a temperature monitoring and controlling system collects data not only about current temperature but location of user inside home as well. The system is also able to detect the outside temperature and set house temperature accordingly. Similarly, the health monitoring system that monitors patient's health parameters in real time also collects data of patient's blood pressure, heart rate, body temperature, etc in real time and stores it. More examples of IOT enabled systems that can generate large amount of data can be traffic management system, emergency services management system, environment monitoring, electrical grid and other utilities and defense. These systems generate data very fast and due to their low processing capabilities they cannot use modern encryption techniques to secure data before sending it across wireless medium where it can be eavesdrop upon.

IOT devices have applications that make it possible for them to collect and store data that can be considered private in nature of the users. If this data is accessed by non recipient or an unauthorized user can cause great damage in more than one way. As of now there is legal framework exists in most countries that can clearly define what data is considered private and collection and use of private data by companies.

However, as the IOT device penetrates further in society and their application domain expands it is quite easy to predict that they will be mining huge amount of data that can be considered personal. It clearly means that people who want to control access to their data will become only harder.

For example if a person enters an area covered with sensor networks his movements the cameras are going to record his/her movements regardless of his/her wishes to be recorded. The only way to avoid this is for the person not to enter area under surveillance.

2. Data Sharing & Interoperability Issues

Due to interconnected nature of IOT devices they are dependent on each other for data transmission and reception. This results in lots of sharing of data as well as devices using data sensed by others. This data usage by devices where data is provided by sensors other then devices own is result of data sharing and interoperability between IOT devices. There are two main issues in here that needs to be paid attention.

The data sharing issue between IOT devices is an important issue. Without a proper data sharing mechanism in place between devices, it is not possible to make devices interoperable. In case of many IOT devices data sharing needs to be done in real time. Data such as weather or health need to be shared in real time for patient monitoring to be possible.

In some cases of IOT devices such as traffic monitoring system, emergency services or electrical grid, there is large amount of data being generated or exchanged. In this case IOT devices with limited power and storage capacity cannot be expected to share all the data that device is sensing for speed that is higher than speed of sensing data. Also, due to its limited processing capacity, it may not be able to process all data.

An example of this can be a health monitoring device that is attached to patient and is monitoring heart rate, blood pressure and temperature of patient. Due to smaller size of this device it may not be able to process or store much of the data that it is sensing, so this device need to upload its data every few hours into another device with higher capacity. Sometimes it can be possible that this device will generate data at more speed than it can be transmitted thus resulting in overflowing of data and wastage of information.

Another facet of data sharing challenge is of data ownership. One type of data is the data sensed by IOT sensor devices. Another type of data that is generated is a byproduct of data sensed by IOT device sensors; this data is mined or generated from sensed data. The challenge here is since the data is generated by actions of user, does it make user the owner of data? A counter argument to this can that since these actions were sensed by an IOT device which recorded data, is the device manufacturer the owner of this data or is it the device owner the owner of data due to transitive relationship of device owning data and the owner owning device?

Interoperability is another challenge that is facing expansion of IOT enabled technology. Interoperability is result of absence of standards in this discipline. There are many device manufactures and each has their own standards, in this case devices of one manufacturer cannot interoperate with devices of the other. This will result in customer having to choose device based on manufacturer and not on its own features. Also this will decrease the competition in market thus limiting customer's freedom of choice.

Some of above mentioned challenges of load balancing during data processing may be solved by load forecasting algorithms [26]. Another challenge of detecting malicious attack may be addressed by an automated forensic investigation system [27].

3. Hardware & Software Issues

Hardware & software related issues in IOT can be divided into two sub issues: i) Issues related to standardization ii) Issues related to failures

A number of objects with embedded systems that can communicate with each other make a network of objects which is referred as IOT. However these objects are often small and hence lack power, processing speed and memory of computers. Now these objects with embedded systems needs to be integrated with Internet, that means these devices need to follow protocols and standards set by the Internet. As it happens, these standards were designed without considering possibility of these kinds of devices getting integrated with Internet one day. These devices mostly consume low power; have limited processing power and memory capacity. These devices also come with option to disable them in order to reduce power consumption.

Also the network that is created by these devices is defined by different set of parameters then wired computer or wireless networks. Some of these parameters are traffic, packet loss, message size and fast changes in topology.

As IOT devices penetrate deeper in our lives, we tend to get increasingly dependent on them for some life critical functions. Some of the applications of IOT devices are home appliances, healthcare, traffic management. These applications are critical ones such that proper function of these applications can make different of life and death for human. For example home appliance devices that manage temperature can malfunction and sudden increase or decrease can affect life of an infant in few hours of time. Similarly, devices that remind patients about their medicine dosages can malfunction due to software/hardware failure. This can result in patient taking high dose or low dose of medicine that can develop into health hazard and result in death of patient. It is also possible that an IOT managing

traffic does not identify an ambulance or fire department vehicles in emergency situations due to various failures that can result in causality of people and damage of property.

IV. CONCLUSIONS

Internet of Things based applications has grown up in every domain due to Internet based infrastructure [28] [29]. However they need certain characteristics such as intelligence, architecture, scalability, complexity in interaction, space and size to get matured. The paper has described all important characteristics for mature IoT based applications. Basically there are three main perspectives on which IoT based research has done so far such as architectural elements, security and applications. Applications require both architectural elements and security so this paper has focused on applications and identified major domain areas of IoT based applications with characteristics. IoT based applications have many challenges associated with them. Issues like data security and breach of privacy are at the core of challenges faced today by IOT research community. A way need to be found that can make secure communication possible between different IOT nodes. A data encryption technique that is light on resources needs to be researched. IOT devices while monitoring can come across a lot of data that can be considered personal in nature hence, laws need to be in place to usability, retrieval and storage aspects of data. An IOT device loses lots of its functionality if its ability to share its collected data is lost. Many IOT devices use data not gathered by them but sensed by some other device and transferred to this device. This is possible only if the two devices are interoperable. Data ownership issues can be sorted out by enacting laws that recognize different owners of data. The device standardization issues are important as it directly affects functionality of devices. The standard for communications were defined before introduction of IOT enabled devices and so it is not possible for IOT devices to adopt these old rules considering their limitations in power, processing capacity and memory capacity. Software and Hardware is not a complete science and this failure can result in very serious, life threatening or death like situations.

REFERENCES

[1] Angelo P. Castellani,Nicola Bui,Paolo Casari,Michele Rossi, Zach Shelby, Michele Zorzi (2010), Architecture and Protocols for the Internet of Things: A Case Study, IEEE, pages-678-683.

[2] BRICKELL , E., C AMENISCH , J., AND C HEN , L.(2004), Direct anonymous attestation, In Proceedings of the 11th ACM conference on Computer and communications security, ACM, pp. 132–145.

[3] Carretero, J. & García, J. D.(2013), The Internet of Things: connecting the world. Personal Ubiquitous Computing .

[4] D. Uckelmann, M. Harrison, F. Michahelles (2011), An Architectural Approach Towards the Future Internet of Things, *Architecting the Internet of Things*, Springer-Verlag Berlin Heidelberg .

[5] Daniele Miorandi, , , Sabrina Sicari, , Francesco De Pellegrini, ,Imrich Chlamtac**(2012)**, Internet of things: Vision, applications and research challenges, Ad Hoc Networks, Volume 10, Issue 7, Pages 1497–1516.

[6] Hasan Omar AlSakran (2015), Intelligent Traffic Information System Based on Integration of Internet of Things and Agent Technology, International Journal of Advanced Computer Science and Applications,Vol. 6, No.2.

[7] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, M. Palaniswami(2013), Internet of Things (IoT) : A vision, architectural elements,and future directions, Elsevier, Future Generation Computer Systems 29, 1645-1660.

[8] Jeong-Yong Byun, Aziz Nasridinov (2014), Internet of Things for Smart Crime Detection, Contemporary Engineering Sciences, Vol. 7, no. 15, 749 – 754.

[9] Lei Li, Jing Chen (2011), System Security Solutions of RFID System of Internet of Things Sensing Layer. J. Net Security Technologies and Application, (6): 34-36.

[10]Liang Shen, Yan Zhang ,JianGu (2012),Development Trend of IPv6-based Information Security Products in Network Layer of IoT. C. In: 27th National Computer Security Academic Communication. (8) :38-40.

[11] Lianos, M. and Douglas, M. (2000), Dangerization and the End of Deviance: The Institutional Environment. *British Journal of Criminology*, 40, 261-278.

[12] Luigi Atzori, Antonio Iera,Giacomo Morabito(2010), The Internet of Things : A Survey, Elsevier, Computer Networks 54, 2787-2805.

[13] Matthew Gigli, Simon Koo(2011) , Internet of Things: Services and Applications Categorization,Scientific Research an academic publisher , Vol.1 No.2.

[14] Mingchuan Zhang,Haixia Zhao, Ruijuan Zheng, Qingtao Wu and Wangyang Wei, Cognitive Internet of Things:Concepts and Application Example, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 3, November 2012.

[15] Nan LIN,Weihang SHI (2014), The Research on Internet of Things Application Architecture Based on Web , IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA),pages-184-187.

[16] PFLEEGER, C. P., AND P FLEEGER , S. L (2002), Security in computing . Prentice Hall Professional Technical Reference.

[17] SADEGHI , A.-R., AND S TUBLE , C(2004), Property-based attestation for computing platforms: caring about properties, not mechanisms. In Proceedings of the 2004 workshop on New security paradigms, ACM, pp. 67–77.

[18] SESHADRI , A., P ERRIG , A., V AN D OORN , L., AND K HOSLA , P. Swatt(2004), Software-based attestation for embedded devices. In Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on , IEEE, pp. 272–282.

[19]S hancan g Li, Kewan g Zhan g (2008),Principle and application of wireless sensor network, China Machine Press .

[20] SIMMONDS , A., S ANDILANDS , P., AND V AN EKERT , L. (2004),An ontology for network security attacks.In Applied Computing . Springer, pp. 317–323.

[21] Vijayakannan Sermakani (2014), Transforming healthcare through Internet of Things, Project Management Practioner's Conference.

[22] Yang Yang (2012), Research and Design of the teaching platform architecture based on IOT , IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.5, pages-103-105.

[23] Zhao Xiaorong1, Fan Honghui1, Zhu Hongjin, Fu Zhongjun1,Fu Hanyu(2015), The Design of the Internet of ThingsSolution for Food Supply Chain, 5th International Conference on Education, Management, Information and Medicine

[24] Zhanlin Ji , Ivan Ganchev , Máirtín O'Droma , Li Zhao and Xueji Zhang(2014) , A Cloud-Based Car Parking Middleware for IoT-Based Smart Cities: Design and Implementation, Sensors 2014.

[25]ZHIBO PANG (2013), echnologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being, Royal Institute of Technology, Doctoral Thesis in Electronic and Computer Systems, Stockholm, Sweden.

[26] Amogha A.K.(2019), Load Forecasting Algorithms with Simulation & Coding, International Journal of Scientific Research in Network Security and Communication, Vol.7, Issue.2, pp.16-21.

[27] P. Santra (2018), An Expert Forensic Investigation System for Detecting Malicious Attacks and Identifying Attackers in Cloud Environment, International Journal of Scientific Research in Network Security and Communication, Vol.6, Issue.5, pp.1-26

[28] Vidhi Tiwari, Pratibha Adkar(2019) Implementation of IoT in Home Automation using android application, International Journal of Scientific Research in Computer Science and Engineering, Vol.7, Issue.2, pp.11-16.

[29] C. Premalatha (2019) Automatic Smart Irrigation System Using IOT, International Journal of Scientific Research in Computer Science and Engineering, Vol.7, Issue.1, pp.1-5.

Authors Profile

Dr.Dharmendra Patel has received his Ph.D degree from Kadi Sarvaviswavidyalaya, Gandhinagar in 2014 in Web Mining area. He has published more than 25 research papers in national and international journals/conferences of repute. He is associated with many international journals of repute as a member of reviewer and editorial board. He has published 2 book chapters in international publisher books. He has published number of technical articles in computer science related magazines such as CSI and OSF. His area of research are Data Science, Web Mining, Image Processing, Fog Computing and Internet of Things. You can reach him by dharmendrapatel.mca@charusat.ac.in.

Dr Pranav Vyas completed his Ph.D.in 2017 from Charotar university of science and technology, changa. He is currently assistant professor at Smt. Chandaben Mohanbhai Patel Institute of Computer Applicatrions, CHARUSAT, Changa. His interests include applied cryptography and network security. He has 10 years of teaching and 8 years of research experience.

Dr. Atul Patel received B.Sc. (Electronics), M.C.A. degrees from Gujarat University, India. M.Phil Degree from Madurai Kamraj University, India. He received a doctoral degree in Computer Science (Wireless Communication) from Sardar Patel University, Vallabh Vidyanagar. Now he is an Associate Professor and Principal, Smt. Chandaben Mohanbhai Patel Institute of Computer Applications – Changa, India. His main research areas are wireless communication, Network Security, Data Mining.

