Internet of Things Device Enabled Smart Home Integrated Architecture with Security Services

J. Deepika[a] **J. Gokulraj**[b]

[a,b]Assistant Professor, Department of Information Technology, Sona College of Technology Salem, Tamil Nadu, India

jdeepikait@gmail.com[a]gokulsct@gmail.com[b]

Abstract— The innovative internet technology of domestic automation applications is widely distributed. Home automation systems have become increasingly sophisticated by providing access to all people irrespective of time or place. Home automation devices, known as smart home systems, are supplied with wireless communication technologies via cell phones and microcontrollers for a remote control of wired non-computers at home. In this digital age, the home automation system was developed to target a broad range of applications for new digital consumers. Smart home systems with Internet connectivity of objects and security services, incorporation of intelligence into sensors and actuators, networking of intelligent elements that enable interactions between intelligent devices allow easy access at different locations, increased calculation power, storage capacity and efficient data sharing.

Keywords—Internet of Things (IoT), Smart Home, Security, Home Automation

1. Introduction

The building blocks of this home automation framework are classic smart home, the Internet and security services. The basic characteristics and technology of each part are found in the proposed solution. Internet of things leads with a range of sensors to internet access and smartphone device remote control. Home-related systems may be fitted with sensors. This translates computer knowledge into home appliances by numerous methods for calculating home specifications and the performance of home appliances. Home automation system allows for the creation, retention, operation, or access of home devices regardless of time and location, with scalable computer resources, storage space and applications

The Home Automation System offers an electrical, sensor, app and net bound network of physical devices. Housing automation is automatic installations, including systems like air conditioning and heating, ventilation, lighting, machinery, and protection system, which are mounted and controlled. Modern systems such as switches, and sensors link through gateways. These gateways are control mechanisms with the gui of the user that communicate with handheld or non-portable devices such as smartphones, mobile telephones, or computers. As domestic parts, automated devices are considered.

2. Related work

Intelligent home is the home extension for building automation which contains all the integrated technologies in control and automation **(Gaurav Tripathi.2014)**. This describes a home that consists of appliances such as lighting, heating, air conditioning, TVs, laptops, entertainment facilities, large household equipment, such as washing machines/dryers, coolers/freezers, surveillance systems and camera systems that can connect and be watched remotely on a time, cellular, smartphone or internet basis. The system consists of wall-mounted terminal or cell-connected sensors and switches connected to a central hub operated by a domestic resident **(Atishay.2011)**.

Auto home system offers, protection, quality of electricity, low costs and comfort. Smart products are installed for comfort and energy savings **(Vittorio Miori.2014)**. These structures are flexible and adaptable to the continually evolving needs of the occupants of the household. The infrastructure is versatile enough to integrate with a number of products and standards from multiple providers **(Yue Li.2013)**. The home automation system architecture provides home estimation, stored data, micro-controller-capable sense sensors for home conditions checks and home-embedded equipment monitoring actuators.

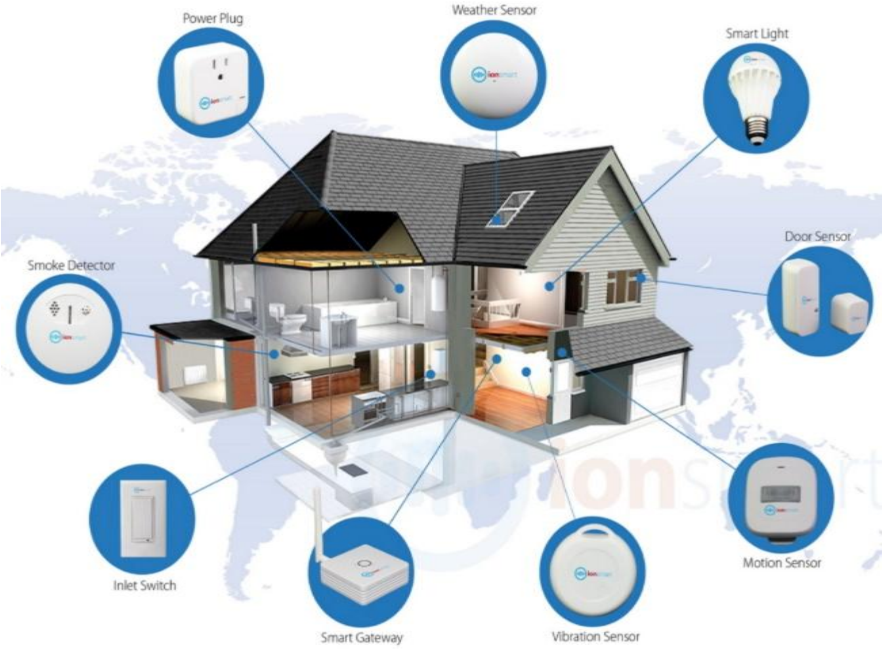

Figure.1 IoT based Home Automation System Features

An irregular scenario is detected (e.g., fuel, smoke, leaking of water, window breakage and the trapped entity in your bathroom), warns are raised, or residents are called up by telephone or Internet, or cameras are triggered in all sensitive locations.

3. Proposed home automation system

Architecture

IoT-based Smart Home Device layout architecture. There are three levels of home automation, for example device layer, network layer and sensing layer. The sensing layer guarantees that data from all household equipment are gathered and transfers data to the middle layer of the network.

For transmitting information to the highest application level, the network layer uses Internet that contains different applications at various levels for several purposes. A type of ARM microcontroller is used for data collection and processing on the sensing layer microprocessor. The Zigbee module built on the IEEE 802.15.4 Wireless protocol is used to transfer the information obtained to the network layer. The power for self-organization can be used to boost system efficiency and deliver improved services across the system network. The above are essential components of autonomy,

- Discovery of the neighbor
- Regulation of media access
- Development of local networking and track
- Management of operation recovery

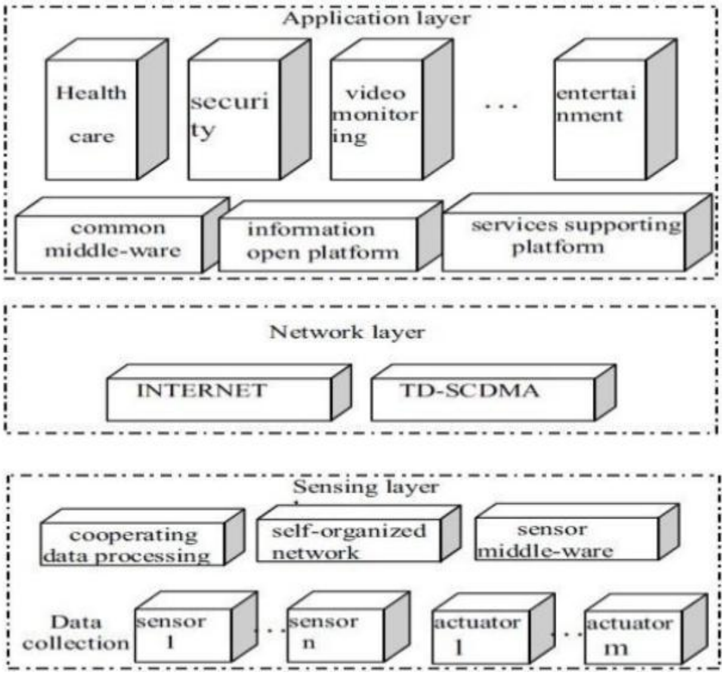

Figure 2. Layered architecture of Smart Home System

B. Sensor Interface

The Wireless Sensor Network (WSN) IoT environment uses the ROM-based Complex Programmable Logic Device (CPLD) to reconfigure the Smart Sensor interface device that combines data storage, data processing and wireless transmission.

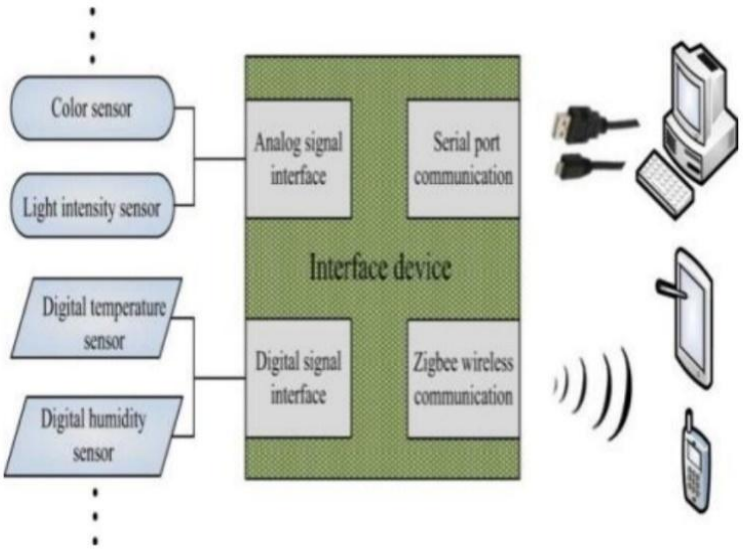

Figure 3. Smart Sensor Interface

With the data collection of several sensor nodes, the wireless sensor network in IoT ecosystem is questioned. When used as interface unit, the microcontroller executes an interrupt feature that doesn't parallel these multi sensor acquisition interfaces with multi sensor data gathering by microcontrollers. Complex Logic Device (CPLD) programmable can acquire parallel multi-sensor data and improves real-time system performance.

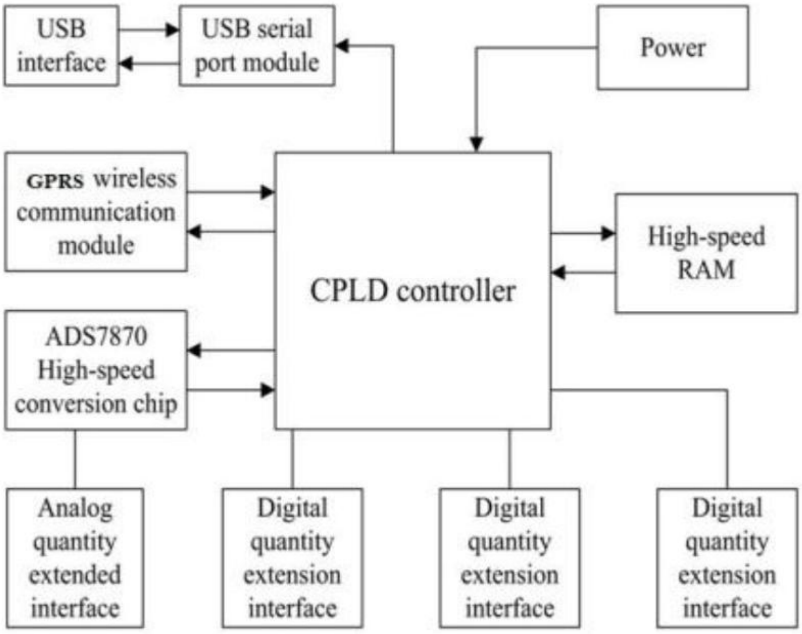
USB interface
USB serial port module
Power
GPRS wireless communication module
CPLD controller
High-speed RAM
ADS7870 High-speed conversion chip
Analog quantity extended interface
Digital quantity extension interface
Digital quantity extension interface
Digital quantity extension interface

Figure 4. Complex Programmable Logic Device

C. *Radio Frequency*

The integrated home system uses an adaptive central controller to establish a radio frequency based on their capabilities for the wireless sensor and the control network. Radio frequency modules, transfer modules, power modules handle non-computing machines of all sorts directly. The intelligent home control system involves computer tracking, managing and maintenance, home security, power statistics and analysis features. Each household system is assigned a single identity with radio frequency identification technology. You may define each system uniquely. The range may be increased or reduced by the radio frequency. Low power and low deployment cost for RFID tags.

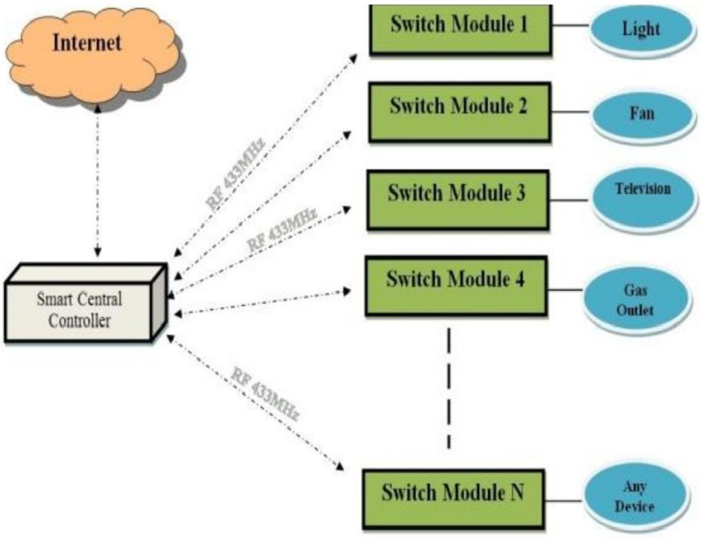

Figure 5.RFID of Home appliances

4. Smart home applications

A. Healthcare

A non-evasively incorporate home control system for the elderly and disabled. These automatic control systems track and avoid the health of these people. Intelligent home management systems devices support the aged and disabled in achieving safe lifestyles. Health monitoring can be carried out remotely by the elderly in smart homes that allow immediate clinical healthcare and make health facilities readily accessible in intelligent homes and in regular homes, without a home control system.

Intelligent homes for the aged fulfill their needs without overt interference from human beings. The intelligent home system allows the aged and disabled people to monitor if their particular care, even on schedule, is met. Health experts monitor the environment inside the household through the use of CCTV for aged persons. Tools that can be relocated to intelligent homes are expressly built to address the needs of seniors and disabled.

Figure 6. Smart Control of Devices

B. Cost Reduction

Residents in intelligent homes use the increased amount of internet products to lower their simple life needs. The remote health observation of older patients and people with disabilities increases access to treatment and lowers health care costs. This method, which is not used in hospitals and clinics, will increase access, and decrease costs in patient care.

In lieu of wireless networks, wireless network infrastructure in smart homes is used to improve reliability and reduce electricity and costs. The safety device uses electricity so it can prevent the malfunction of any computer that can waste resources and lead to a larger consumption of energy. The energy system is integrated for energy saving without citizen interference.

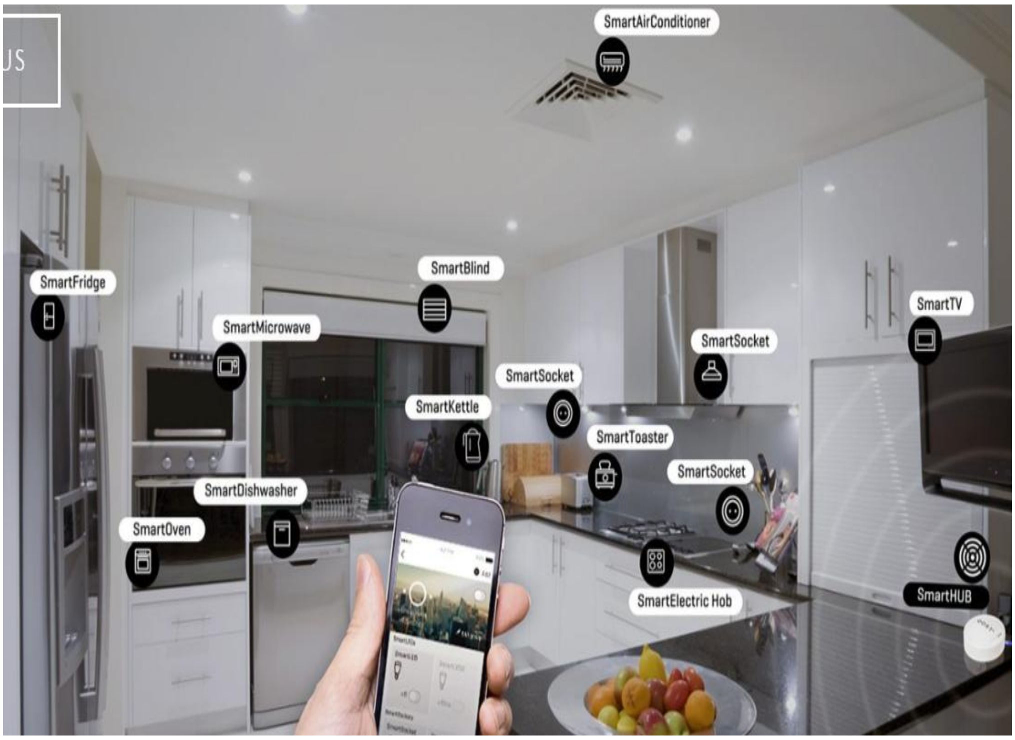

Figure 7. Smart Kitchen

C. Energy Conservation

Intelligent home solutions use smart devices to monitor intelligent processes and reduce energy consumption by advanced technologies. These instruments can contribute to improvising energy conservation performance and energy usage. The intelligent home lighting systems provide automatic LED light control. These devices are used primarily to allow and uninstall automatic lights. Lighting systems optimize electricity self-produced and reduce energy efficiency. Self-produced solar energy can be usable at daytime.

Standby machines may be automatically shut off at night or when they are not operational to reduce electricity consumption and conserve energy for potential use. When people vacate or leave their homes in order to minimize electricity consumption, the Internet of things equipment works automatically in the home control grid. Temperatures fluctuate continuously inside and outside the home, resulting in a spike in energy demand at certain times. Consider a scenario in which indoor temperature can be controlled by air conditioning systems and the low energy factor intake offers a relaxing atmosphere.

D. Convenience

Home automation control systems in intelligent homes provide residents with additional ease, guarantee their protection and security and often allow gadgets that are added to the advantages of the system to be operational. All these systems are integrated with several sensors and wireless networking operations. For e.g., when people are not in their clever houses, computers automatically turn off in their homes.

Residents can still pay their bills quickly and can use paper keys rather than smart devices. Without needing to present the user in the actual world, it is possible to operate the home operated System using handheld devices or remote control. The power can be unified for all facilities, which does not complicate its use. This helps the user to conform to the governing network's user interface.

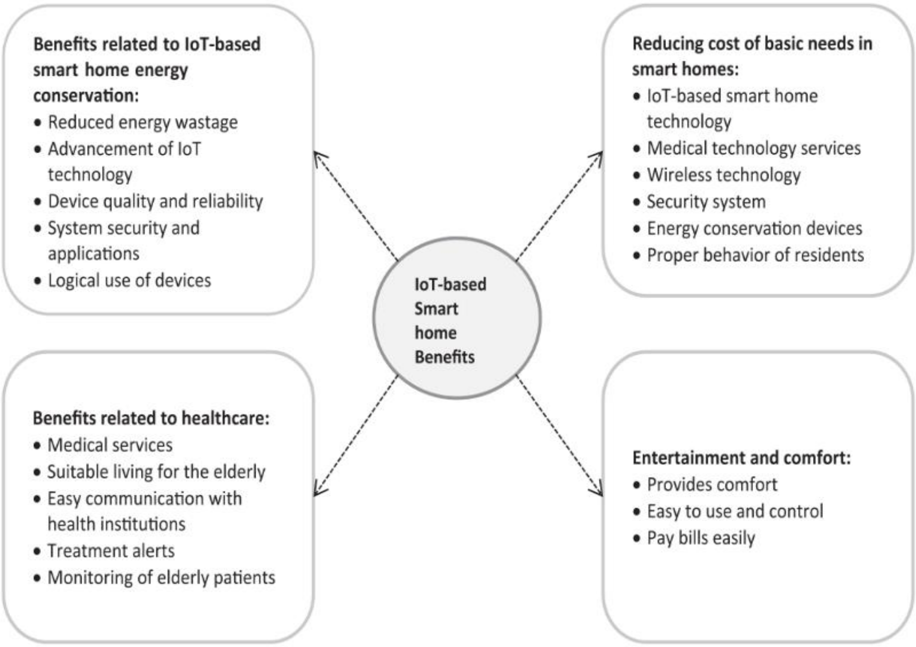
Benefits related to IoT-based smart home energy conservation:
• Reduced energy wastage
• Advancement of IoT technology
• Device quality and reliability
• System security and applications
• Logical use of devices
Reducing cost of basic needs in smart homes:
• IoT-based smart home technology
• Medical technology services
• Wireless technology
• Security system
• Energy conservation devices
• Proper behavior of residents
IoT-based Smart home Benefits
Benefits related to healthcare:
• Medical services
• Suitable living for the elderly
• Easy communication with health institutions
• Treatment alerts
• Monitoring of elderly patients
Entertainment and comfort:
• Provides comfort
• Easy to use and control
• Pay bills easily

Figure 8. Smart Home Benefits

5. Security services

A. Authentication

The authentication process enables different integrations devices deployed in various contexts on the internet. The authentication process involves authentication of routing devices which require data transport and authentication of the data route source in the network. Enhanced key deployment and control challenges prevail in the authentication phase of computers. Cryptography algorithms need not be a big overhead for the key generation and key exchange strategies on heterogeneous network nodes. The encryption and decryption process is the required methods for the validity of cryptographic keys and the integrity of key transactions that support the authentication of exchanged messages.

B. Authorization

Authorization requires requirements of rights of access to various services and access control systems caninclude only approved entities with access rights. Any internet device illustrates restricted methods for confirming connectivity to a heterogeneous network, which may vary from other connected internet devices to the same node. In the heterogeneous internet of things network, the design and operation of multiple permit and access control strategies for the different node capacities must be deployed.

C. Privacy

The use of independent artifacts in the Internet of personal data, such as health data, introduces a new degree of danger to the confidentiality of users. Without really knowing it, the Internet of Stuff nodes gathers personal information. The strategies provide user-centered data security, content-oriented data protection and context-oriented privacy.

But the network of stuff includes self-contained nodes, which gather information and involve data security models directed towards objects. In addition, much of the privacy law mandates reminding consumers of the management and administration of sensitive data. It is a challenge in a heterogeneous setting to recognize nodes which can access passively acquired private user information.

6. Results and discussion

A. User Recommendations

The operating behavior of certain devices in heterogeneous networks can be utilized for prediction with the ability to properly use devices and the operating times.. Users should commit to a set runtime to effectively reduce power consumption and the costs of household appliances. The house automation control systems' energy services are integrated to respond to queries concerning household device power use data by conducting energy consumption analyses on household devices, and to improve household energy consumption recommendations. The networking of stuff devices between Internet is helpful for defective diagnostics and home diagnostic systems with semantic query systems that deal with the failure of heterogenic network nodes.

B. Healthcare recommendations

Healthcare institutions and associations offer assistance and advice and provide the standard of smart homes and healthcare with medical uses. Health institutions supply elderly people at home with the right guidance, for example by means of interactive tutorials. Patients are remotely consulted in intelligent homes, providing treatment guidelines, patient diagnosis and aging and disability assistance.

C. Safety recommendations

Guidelines are provided for the maintenance of fire systems and electrical equipment used in smart homes. A recommending framework for handling IoT network connectivity between IoT computers, networks and operating strategies implements suitable systems detects errors in intelligent households and advises using household appliances. A hardware protection module used in intelligent homes in order to improve the security of the devices and to make data transmission between devices effective.

For stable data sharing, processing and preventing loss of data during data transmission within the network of objects, the privacy scheme in heterogeneous networks within automated control rooms is recommended. In order to include guidance and forecasts in various scenarios a suggestion framework would be introduced for smart homes. The technology estimates consumer requirements based on the past experience of product use in home automation. For instance, if a person uses two identical devices, for example a DVD player and a music player, concurrently. The framework makes suggestions on the user's actions.

7. Conclusion

Linked equipment that lets households and utilities save money, improve home comfort and energy quality while greening it. The security services added by the device allow the collecting and monitoring of private information from the customer. Continuing to build the internet of heterogeneous stuff and the convergence of linked networks of artificial intelligence technology would help to establish an intuitive ecosystem in a modern household that predicts what the inhabitants need or expect and delivers user interface effortlessly.

References

1. GauravTripathi, Dhananjay Singh, and Antonio J. Jara, “A survey of Internet-of-Things: FutureVision, Architecture, Challenges and Service”, IEEE World Forum on Internet of Things (WF-IoT),2014, pp. 287-292
2. Vittorio Miori, and Dario Russo, “Domotic evolution towards the IoT”, 28th International Conference on Advanced Information Networking and Applications Workshops, 2014, pp. 809-814
3. SaritaAgrawal, and ManikLal Das, “Internet of Things – A Paradigm Shift of Future Internet Applications”, International Conference on Current Trends in Technology, December 2011
4. Arjun P. Athreya, and Patrick Tague, “Network Self Organization on the Internet of Things”, IEEE
5. International Workshop of Internet-of-Things Networking and Control (IoT-NC), 2013, pp. 25-33
6. Yue Li, “Design of A Key Establishment Protocol for Smart Home Energy Management System”,Fifth
7. International Conference on Computational Intelligence, Communication Systems and Networks, 2013, pp.88-93
8. Atishay, J. Ashish, T, “Architecture for High Density RFID Inventory System in Internet of Things”,
9. Proceedings of International Conference on Computer Science and Information Technology, Springer 2011.
10. Bhole, M., et al., “Delivering analytics services for smart homes” Proceedings of IEEE Conference on Wireless Sensors (ICWiSe), 2015
11. Chao-Lin Wu, Yi-Show Tseng, and Li-Chen Fu, “Spatio-Temporal Feature Enhanced Semi-Supervised Adaptation for Activity Recognition in IoT-based Context-aware Smart Homes”, IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, 2013, pp. 460-467
12. M. Al-Qutayri, H. Barada, S. Al-Mehairi, and J. Nuaimi, “A Framework for an End-to-End Secure Wireless Smart Home System”, IEEE International Systems Conference Montreal, Canada, April 7- 10, 2008
13. Y. Yang, H. Cai, Z. Wei, H. Lu, K.-K.R. Choo, “Towards Lightweight Anonymous Entity Authentication for IoT Applications” Springer, 2016, pp. 265–280.

14. E. Bertino, K.-K.R. Choo, D. Georgakopolous, S. Nepal, “Internet of Things (IoT): smart and secure service delivery”, ACM Trans. Internet Technol. 16 (4) (2016) pp 1–7
15. J. Deepika “Improved Clustering with Optimization and Intelligent Path Selection” International Journal of Innovative Technology and Exploring Engineering, Volume 9, Issue 4, pp 2310-2313, February 2020.
16. S.R. Moosavi, T.N. Gia, E. Nigussie, A.M. Rahmani, S. Virtanen, H. Tenhunen, J. Isoaho, “End-to- end security scheme for mobility enabled healthcare Internet of Things” Future Gener. Comput. Syst. 64 (2016) pp 108–124.
17. F. Li, J. Hong, A.A. Omala, “Efficient certificateless access control for industrial Internet of Things”, Future Gener. Comput.Syst. (2017).
18. J. Lopez, R. Rios, F. Bao, G. Wang, “Evolving privacy: from sensors to the Internet of Things” Future Gener. Comput. Syst. 75 (2017) pp 46–57.
19. J. Deepika, J. Gokulraj, S. Srisharaan, S. Shasang “Enhanced Technique on Augmented Reality and Virtual Reality with Brain computer interface in Education” International Journal of Advanced Science and Technology, Volume 29, Issue 7, pp 12185 – 12190, 2020.
20. M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, K. Wehrle, “A comprehensive approach to privacy in the cloud-based Internet of Things” Future Gener. Comput. Syst. 56 (2016) pp 701–718.
21. S. Raza, T. Helgason, P. Papadimitratos, T. Voigt, “Secure Sense: End-to-end secure communication architecture for the cloud-connected Internet of Things”, Future Gener. Comput.Syst. (2017).
22. J. Gokulraj, Dr.J. Senthilkumar, Dr.Y.Suresh, Dr.V.Mohanraj, “Data consistency matrix based data processing model for efficient data storage in wireless sensor networks” Computer Communications, Elsevier, Volume 151 pp 172-182, 2020