ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

Applications and Challenges in IoT based Smart Homes

Brijendra Singh
School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, 632014, Tamil Nadu, India.

Muhammad Zubair Khan
Department of Computer Science, Taibah University, Madinah, Saudi Arabia.

Senthil J*
Department of Computer Science and Enginnering, Nandha Engineering College, Erode, Tamil Nadu 638052, India.
senthil.j.vit@gmail.com

Abstract:

With the advancement of the internet, embedded devices and wireless sensor technologies bring a significant development in the Internet of Things (IoT) for smart homes. Smart homes are intelligent buildings mounted with powerful sensor devices that help individuals remotely monitor the building activities to make smart decisions. IoT connects individual things or objects in a smart home environment that communicates with each other over the internet. Applications of IoT-based smart homes have drastically increased in the past few years with an eco-friendly environment. This article gives an overview of various applications of IoT-based smart homes. Besides, it identifies various challenges associated with the successful implementation of IoT-based smart homes. Also, it identifies some of the approaches to find a solution to these challenges. We then identify the unsolved problems for the researchers towards smart-home automation. This review shows that most of the IoT-based smart home applications are based on energy-efficient and security-based approaches. Major challenges identify as human motion detection, scalability, lack of global standards, interoperability, data processing and management, mobility management, resilient architecture, device connectivity, and services at affordable cost based on the literature.

Keywords: IoT; smart home; automation; energy; remote monitoring

1 Introduction

The smart home's idea is derived from an intelligent environment that collects and applies the surroundings' knowledge to make intelligent decisions for providing more human-centric home services. Smart home-based services allow individuals to keep track of various home activities remotely, like monitoring their children, parents, pets, and household things. Further, it provides various advantages in an enhanced secure home environment, comfort, energy-saving, and cost minimization. IoT-based smart home systems improve the lifestyle of an individual by connecting different digital devices. Smart homes are automated buildings installed with various sensor and control devices that form a wireless sensor network. These control devices are communicating with the help of a common platform called gateways. These devices' sensed data are forwarded to these gateways, interacting with the user interface using mobile, tablets, and personal computers. IoT facilitates managing connectivity between various devices and gateways [1]. In a smart home-based IoT environment, the interaction between home appliances and sensors plays a vital role. Hence, various security-based wireless protocols for the smart home-IoT system identified [2] are EnOcean, Thread, Z-wave, KNX-RF, and Zigbee. All of these protocols follow some security mechanisms like encryption and authentication processes.

The development of advanced technologies like pervasive and ubiquitous computing, which provides professional services to anyone, anytime and anywhere, cloud and fog computing; provides a way for data storage and its security, big data analytics, and blockchain technology has opened the way in the development of IoT based smart home services and applications. Additionally, it facilitates future researchers to understand various applications and implementation challenges. This paper acts as a base for researchers to further develop IoT-based smart home solutions and fix the implementation challenges. The smart home architecture is illustrated in Fig. 1.

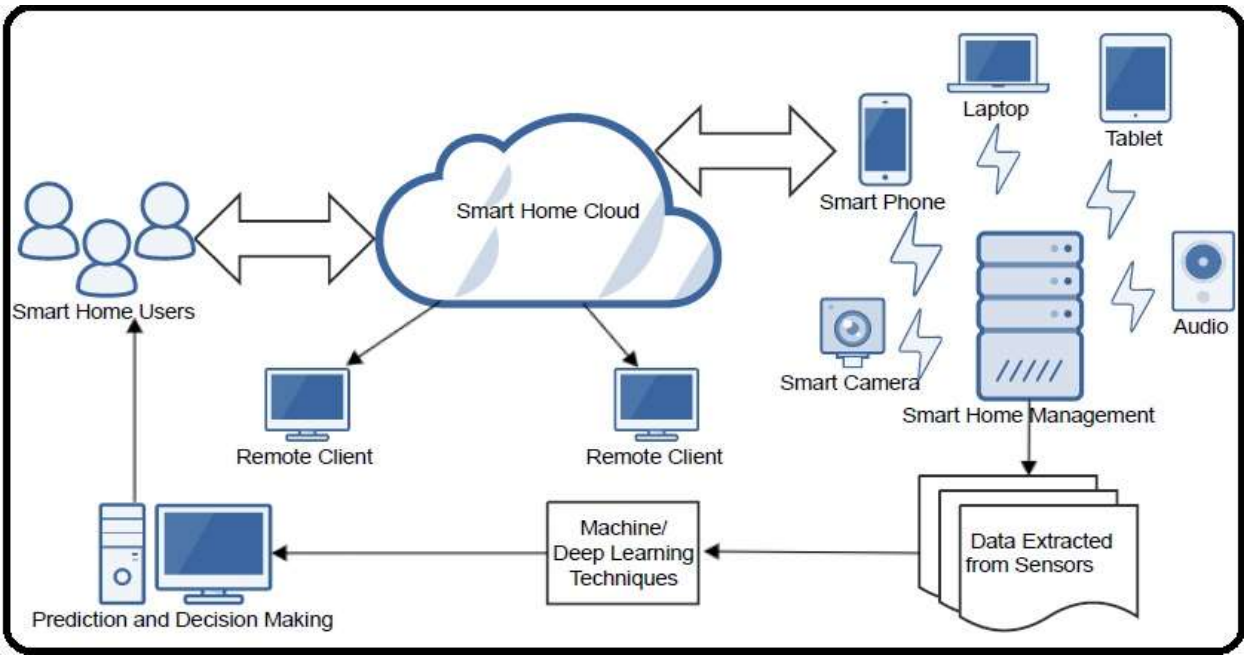

Figure 1: Smart home architecture

This research article is organized as follows. Following the introduction, various applications of IoT based smart home is presented in section-2. Various implementation challenges associated with IoT-based smart home development is presented in section-3, followed by a conclusion in section-4.

2 Applications of IoT based Smart Home

This section enlightens various applications developed by researchers with their advantages. We reviewed most of the applications based on current research. Tab. 1. represents the various applications and their advantages by multiple researchers for a better understanding of the readers.

Table 1: IoT enabled smart home applications with its advantages

Ref. No.	Applications	Advantages
[3]	Smart home IoT based monitoring and control system	Flexibility, Efficient energy consumption, Safety of people, Improved quality of life
[4]	Multilayer cloud-based architecture and security service framework for IoT-based smart homes	Effective communication between diverse nature devices, Secure environment for communication
[5]	Automated smart home IoT based secure system	Energy-efficient data encryption
[6]	A smart home energy management system using IoT and big data analytics	Energy utilization, remote monitoring
[7]	IoT based gateway architecture for a smart home environment	Automated security approach
[8]	Innovative smart home system powered by botanical IoT and emotion detection	Green-living environment, smart living environment
[9]	HEMS (Home Energy Management System) based on the IoT smart home	Efficient energy utilization, Mobile Environment
[10]	IoT based smart home security system	Door management
[11]	Framework for smart home-based IoT	Effective management and communication among heterogeneous devices
[12]	Customary homes to smart homes using the Internet of Things (IoT) and mobile application	Energy-efficient, flexible, extensible, automated
[13]	Smart-home automation using IoT-based sensing and monitoring platform	Flexibility, Remote Monitoring, Smartness

[14]	The IoT-based intelligent approach of the smart home environment for fire prevention and safety	Energy-efficient approach, Best Accuracy

A smart home IoT-based monitoring and control system is developed [3] using Frugal Labs IoT Platform (FLIP). The FLIP architecture consists of four layers: the device layer, gateway layer, cloud layer, and application layer. In a proposed smart home network system, various home appliances are connected to the FLIP device. Further, the FLIP device is connected to the internet with the help of a FLIP gateway. This gateway plays an important role by introducing a security layer to make the smart home system more secure. Essential information from the smart home environment is sent to the server to control the home ecosystem. FLIP is an open-sourced computer platform that Frugal labs, Bangalore, India, develop. This smart home aims to improve people's quality of life, security, and safety with efficient energy consumption. The proposed system is more flexible and can be altered based on the user's requirements. Another multilayer cloud-based architecture is proposed [4] to enable effective communication between diverse nature devices offered by various vendors. Further, to overcome heterogeneity issues, an ontology-based approach is proposed to support a secure environment for communication.

An automated smart home IoT-based secure system is developed [5] using a Triangle-based security algorithm (TBSA). Wireless sensor network (WSN) is used to enable the connection among various devices. WSNs are clubbed with internet protocol to develop IoT applications. The challenges in WSN are addressed by introducing a secure algorithm. TBSA enables energy-efficient data encryption for providing a secure, IoT-based platform. Energy consumption in TBSA was found to be very less as compared to other existing security techniques. The integration of low-power Wi-Fi with TBSA in wireless sensor networks provides various benefits like adding more sensor nodes, more coverage range, and efficient data encryption using TBSA. The proposed system is verified for various security requirements like data and system security. Further, the proposed secure IoT-based system can be implemented in other application domains too.

Energy utilization is one of the main goals for IoT-based smart home systems for monitoring and controlling home appliances. An energy-efficient solution for a smart home environment is proposed [6] using the internet of things and big data analytics techniques. In this energy management system, each device in the home is integrated with a data acquisition system that collects data from each device about requirements and sent it to a central server for further processing. The designed system is tested and validated with the help of a case study. With the help of a mobile application, users can easily monitor and control various devices remotely.

An IoT-based gateway architecture is proposed [7] for the smart home environment. Auto management in a smart home is supported by auto configuration and auto-updation. System security is achieved by auto-configuration, while auto-update is needed to manage to persist system security requirements. Security needs for smart homes based on IoT platforms are different as compared to the mission-critical system. The security management is largely depending on configuration and installation by inexperienced staff. It is recommended to automate this process to make these security requirements more effective. Therefore, an automated security approach is presented for solving such problems.

To make a smart living environment, botanical IoT with a smart home is analyzed [8]. A smart home 2.0 system, an advanced smart home 1.0 based on a green environment, is designed and implemented. The communication between home and greeneries is enabled with a mobile-based cloud system for data collection management and visualization purposes. A user feels tired while returning from work. Smart home with greenery helps him to feel good and relax. Hence, a smart home 2.0 solution is proposed, cultivating and managing such a green environment. This is achieved using sensor devices in a green environment to monitor various parameters like temperature, humidity, sunlight, light intensity, and carbon dioxide. Sensor devices monitored all these parameters and sent them to a cloud server that offers different services like sensor device management and user authority management. The user uses a mobile-based interface to access the cloud to accomplish their needs. Smart home 2.0 architecture deployment consists of various phases like greenhouse building, configuration installation of botanical sensor networks, and construction of necessary cloud platform.

An IoT-based home energy management system model [9] is built to efficiently utilize energy in smart houses. The system consists of a control server, various devices, and sensors. The control server controls the data that comes from these devices and sensors. The home energy management system keeps track of each device and sensors for its optimal energy consumption. It controls it by activating and deactivating data flow from various devices and sensors. These sensors could be image sensors, environmental sensors, infrared and ultrasonic sensors. The developed system for efficient energy utilization can be controlled and managed by administrators or users in a mobile environment.

A secure home-based system using IoT is proposed [10] for door management/accessibility and voice alert remotely with a smartphone's help. The visitor's image is captured at doorsteps, and an alert is sent to the user's email. It is a wireless system to authenticate visitor's doorstep. The house door's access is enabled after successful authentication of visitors using an electromagnetic door lock module. The proposed system consists of Raspberry Pi, Raspberry Pi Camera, Passive Infra-Red sensors. Another framework for smart home-based IoT is proposed [11] for effective management and communication among heterogeneous devices. This framework uses different programming methods to make this approach more effective and implemented as a web service.

A smart home automation system [12] based on IoT is designed to control home appliances and various devices remotely with an Android-based smartphone. More specifically

system is designed, which is more energy-efficient, flexible, extensible, automated using IoT, which consists of cloud-based networking and various communication protocols-based standards. It enables the user to control different home devices at remote locations with a user-friendly interface. The proposed system compromises two stations called the base station and satellite station. The base station is an Arduino mega microcontroller that is connected to Wi-Fi for internet accessibility. It communicates with the satellite station using an RF transceiver module. The satellite station used various sensors to collect necessary data to detect gas leakage, temperature, motion, and touch. This data is used to manage and control home appliances and devices.

A smart home automation system based on IoT is designed [13] to provide visual, thermal, and hygienic comfort to users. Another smart home system task is monitoring, controlling, and analyzing various data collected from sensing devices to provide intelligent automation by controlling the devices remotely. EmonCMS cloud server platform is used to collect and analyze data for controlling the home devices remotely. Real-time monitoring, sensing of data, downloading, and uploading data from cloud servers are performed using a microcontroller board. The proposed design is very flexible and can be applied to large buildings by adding more sensors. In the future, more smartness could be added by introducing more functionality using advanced AI techniques.

Fire detection in a smart home environment is a critical issue and can be avoided to stop unwanted death and property loss. The existing fire network system based on wireless sensor networks fails to detect fire multiple times due to sensor failure. An energy-efficient approach is proposed [14] based on WSN with multiple sensors for the best accuracy of fire detection at the earliest. False alarms are avoided using a global system for mobile communication (GSM) technology. It is proved using a simulation system that the proposed approach is successfully detecting fire at early stages even if the sensor is not working.

3 Implementation Challenges

We present a brief review of recent work done in reliable data transmission in IoT networks. The three major areas related to reliability include efficient resource allocation, latency management, and security. The following subsections discuss the literature review in these three key areas.

3.1 Privacy and Security

The large number of devices are connected to the internet in a smart home environment is increasing. Therefore, there is a potential risk of malicious attack. Security in the smart home environment is a critical issue since it involved people's confidential and personal information. Most of the devices launched in the market are more focused on connectivity but lack security and are easily attacked by hackers. Six requirements of smart home security and privacy are confidentiality, integrity, availability, authenticity, authorization, and non-repudiation [15]. Security attacks can be categorized in two different ways i.e, passive and active attacks. In passive attacks, the third party steals the information without making any changes in the data.

On the other hand, active attacks will make some modifications or addition in the system data. However, passive attacks are more dangerous since it is not easy to detect them instead of preventing such attacks. Preventing such devices in the smart home environment from such attacks is a great challenge and should be addressed to save the digital economy. However, many researchers have come forward to provide more privacy and security solutions in smart home settings [16-19]. Data is transmitted in IoT-based environments to be more vulnerable to major attacks by intruders in wireless networking. Hence, IoT needs the implementation of security mechanisms but at the same time to ensure cost-effective strategies.

3.2 Human Motion Detection

Human motion detection is one of the potential challenges in the smart home living environment. Deep learning techniques such as convolution neural networks and recurrent neural networks are applied on time series data obtained from sensors for human motion detection by developing human behavioral models. Many researchers showed the effectiveness of these techniques in human activity detection. However, wearable technologies, sensors, and cameras play an important role in reliable data collection. Implementation of sensor technology efficiently might be a future challenge towards human activities detection. Various efforts are made by researchers towards the analysis of human activity detection in the smart home environment [20-23]. Human motion detection is crucial for older people to protect them from falling. The researchers should investigate new machine/deep learning approaches for human activity detection in an efficient manner. At the same time, we can monitor human activities in a real-time environment. For any human activity recognition, two aspects are essential. The first one is to identify the human activities, and another one is to make the prediction based on those activities. Machine learning techniques can be helpful to solve these two aspects.

3.3 Scalability

Scalability is the property of the cloud to accommodate the growing number of smart homes based on specific requirements. Fog and cloud computing technologies supports scalability and flexibility of resources in smart home IoT based environment. However, various researchers provide a scalable solution towards IoT-based smart homes. Low cost and scalable solutions based on multiple sensors [24] are proposed to improve indoor quality. Another scalable architecture [25] based on IoT-based smart homes is proposed to handle huge amounts of data and reduce the system's complexity. However, a comparison [26] between cloud and fog computing shows more scalability in fog computing because, in the cloud, the deployment of new data centers is cost-bidden.

3.3 Lack of Global Standards

IoT-assisted smart home environment involves various stakeholders like devices and various cloud service providers. Therefore, the lack of global standards is still a challenge to make a smart home environment simpler, cost-effective, compatible among stakeholders. Global standardization is very much required to provide efficient home-based cloud services to manage various system resources. Lack of standards in IoT-

based smart home solutions remains a great challenge because of the heterogeneity of connecting devices and fractured solutions. Technological solutions can be useful to make global standards in IoT-based solutions. However, very few researchers attempt to study global standards for interoperability and security [27]. Different device manufacturing companies should be more focused on how to standardize and provide another framework. At the same time, users have to decide to select a compatible device with the existing communicating devices [28].

3.5 Interoperability

Interoperability is the ability where two or more systems can exchange the information without any difficulties. Interoperability issues arise in IoT-based smart home solutions, which each of them provides its infrastructure, devices, data standards, and protocols. Smart home interoperability is a significant challenge [29] in terms of communication, connectivity, and integration protocols. Lack of global standards and proprietary communication protocols for devices leads to a lack of interoperability in the home automation system. Further, these interoperability issues create significant problems such as the development of cross-platform IoT-based architecture, incompatibility of devices with other devices, and finally stops the large-scale integration of IoT-based solutions.

However, different interoperability solutions are proposed by researchers to facilitate IoT vendors to share information and work together. An interoperability framework [30] with selected characteristics is proposed for smart home communication protocols to facilitate working with different IoT platforms. Another self-evolving algorithmic approach for data interoperability in IoT systems is proposed [31] in an IoT environment. A multi layered cloud architectural model is proposed [32] for handling interoperability issues in heterogeneous IoT-based platforms[46]. However, various solutions are proposed for a specific perspective of interoperability, but very few consider different perspectives. IoT device capabilities should also be considered while solving the interoperability issues. Also, it is essential to connect other platforms and capacity to add more platforms in the future for the smart IoT ecosystem [33].

3.6 Device Connectivity

Various household devices can be connected to provide a more efficient way for data exchange. To understand the system's current state, we need multiple sensors to communicate with each other seamlessly for helpful information exchange. However, the communication of these devices and sensors will be decided by the appropriate communication protocols. Further, these protocols can be categorized into three categories such as wireless, wired, or hybrid. Some of the wired communication protocols are Ethernet, X10, Universal Powerline Bus (UPB), INSTEON, Multimedia over Coax (MoCA), and KNX and wireless protocols are Wireless Fidelity (Wi-Fi 802.11n), Bluetooth, Bluetooth LE, ZigBee, Z-Wave, and 6LoWPAN [34]. A framework for seamless device connections in a smart environment is proposed [35], which ensures interoperability across all the devices. Still, researchers expect much research to solve device connectivity issues such as security and privacy.

3.6 Affordable Cost

As the number of devices increases in IoT-assisted smart home environments, efficient communication between them to share the information over sensory networks becomes important with affordable cost. Energy-efficient devices based on low power solutions and efficient resource utilization leads to reasonable implementation cost over interconnecting networks. Affordable price plays a vital role in converting traditional house to intelligent house. Therefore, it is essential to make sensor devices more energy-efficient and automated, reducing overall implementation costs. Low-cost long-range (LoRa) is one of wireless technology which provides solution a low price. Various solutions are proposed by researchers based on affordable cost. A wind-driven bacterial foraging algorithm [36] is proposed and devised as a strategy based on monitoring power consumption in IoT buildings and home appliances. Another application [37] of intelligent home automation based on the low cost, which integrates software and hardware, is implemented successfully. Another application [38] that uses Bluetooth-Low-Energy with fuzzy approaches in intelligent home automation systems showed the best performance. More research is needed to find more cost affordable smart home solutions for the extensive integration of IoT.

For a better understanding of readers, the IoT enabled smart home challenges and solutions presented in Tab. 2.

Table 2: IoT enabled smart home challenges and solutions

Ref. No.	Challenges	Solution	Evaluation Matrices
[16]	Privacy and Security	Results in the form of contextual and design factors for future privacy designs	Future research can be focused on critical evaluation of design
[17]	Privacy protection of access policy	Blockchain based secure authentication mechanism	Evaluated based on the usage to demonstrate its practicality

[18]	Heterogeneity issues in the presented layered cloud platform	Ontology-based security service framework	Public keys and ID's, Signature algorithms
[20]	Triaxial Acceleration-based Human Motion Detection	Provided with the help of statistical features	Radom forest algorithm
[21]	A Wrist Worn Acceleration Based Human Motion Analysis	Using multiple features and random forest	Through recognition data sets
[22]	Wearable Sensors for Activity Analysis	Sequential Minimal Optimization based random forest	Through two benchmark datasets
[23]	WiFi-Based Smart Home Fall Detection System	Recurrent Neural Network	Comprehensive experiments on real-world dataset
[24]	IoT based Smart home for enhanced living environment	Low cost and scalable multi sensor based smart home solution for improving living environment	Validation through scalability, reliability and easy installation
[25]	Scalable big data analytics	A scalable architecture solving the problem of scalability and complexity issues	Sensor-based technologies
[30]	Achieving interoperability in smart homes	Developed an interoperability framework for smart home communications protocols	Real communication technologies
[31]	Facilitate data interoperability in IoT environment	Self-evolving intelligent algorithms	Self-learning and incremental learning intelligent algorithms
[36]	Cost effective management for smart IoT networks	Wind-driven bacterial foraging algorithm	Binary particle swarm optimization, genetic, genetic wind driven optimization, and genetic binary particle swarm optimization algorithms

Different challenges [4] are identified as security, privacy, scalability, lack of global standards, and performance. These challenges could be solved with good collaboration between government organizations, cloud service providers, smart device-making companies, and standard organizations. The research identifies and discusses multiple challenges [39] involved in IoT-based smart homes: interoperability of communication protocols and data processing. Advanced big data analytics approaches are needed to handle huge amounts of data generated by IoT devices. The current problem is effective communication between various devices because of the use of diverse protocol standards. There is no doubt [4] that the integration of IoT with the cloud provides the best platform for smart home development to make people feel more comfortable and enjoyable. Lack of such a smart home ecosystem is found. Further, it is recommended to develop a well-defined approach towards new IoT architectures and operating services.

Various research problems [40] related to IoT implementations for smart homes are identified as marketing, device connectivity, security, safety, and energy consumption. Smart wearable technology might be the future of smart home IoT-based systems powered by various sensors. Research challenges are to develop more smart home applications that can connect these smart wearables, gadgets and control them based on real situations.

A study [41] has been done to find the user's acceptance of smart home-based services. Results revealed that security issues prevent consumers from smart home services acceptance. A proper organizational and technical infrastructure is required for users to accept smart home-based services. Delivery of efficient services at any time should be provided to the consumers to realize the actual benefits. These results are obtained after applying the value-based adoption and technology acceptance model.

Security issues in IoT –based smart home environments are analyzed [42]. Since most of the smart home devices are connected with real-world objects and incidents. Hence, the chances of miss happening are more. Therefore, a more secure environment should be provided while delivering smart home IoT-based services. Some of the security threats identified are trespass, denial of service (DoS), distributed denial of service (DDoS), falsification and monitoring, and personal information

leakage. The attacker can hack the door's smart lock, and he can trespass on the home without damaging the door lock. To avoid this attack, the smart door should have a strong password and change frequently. Denial of service is an attack on a networking device and illegally accessing it in a smart home environment. We can use authentication methods to identify and block unauthorized devices. Routing tables can be altered in a gateway, and information can be altered and leaked, falsity the confidential information. This attack can be prevented using a secure socket layer method with suitable authentication techniques and block the unauthorized device to access the smart home network. Safety of concern in a smart home is the main issue. Different sensors accomplish the monitoring of various devices in a smart home. These sensors could be attacked by attackers directly, and the device can be infected. To avoid this attack, encryption between gateways and sensor devices can be applied. These security measures help companies to provide various smart home applications with the safety of concern.

A systematic review [43] has been conducted based on remote health monitoring for smart home IoT-based systems using body sensor networking. The security risk and other requirements related to telemedicine in healthcare for smart home-based IoT systems are analyzed. Challenges in telemedicine for smart home-based IoT systems are identified. For smart home users, their safety and privacy are still an issue. The open challenges are self-management, patient privacy, data management, and resilient architecture[47]. The collaboration between academia and industry must rectify security issues in telemedicine and health monitoring using IoT. Vendors and service providers are also responsible for providing security standards for devices. Further, users are also responsible for security attacks. They should be aware of possible security attacks for their devices like tablets, mobile phones, personal computers, electronic gadgets, and mechanisms to avoid these attacks.

Different requirements [44] of smart home-based IoT systems are mobility management, channel security, consistent data rates, and handover support. Mobility management is a major problem in the Wi-Fi network and classifies as location and handoff management. One of the approaches to resolve the mobility problem is proxy mobile IPV6 (PMIPV6). Security issues in route optimization still exist while the protocols belonging to PMIPV6. To keep in mind these issues, a new protocol is proposed to deal with security issues in route optimization for smart home-based IoT solutions. Proposed protocols use the Diffie-Hellman security algorithm for session key exchange. Further, the correctness of the proposed protocol in PMIPV6 is verified using various approaches and a network simulator. Future research could be the extension of the developed protocol for mobility management in a distributed environment under a 5G network.

With the advent of various smart devices and IoT related devices, there are challenges [11] in a smart home-based IoT environment to communicate all these devices due to the diverse requirement of the smart home. An extensive review [45] has been conducted to analyze challenges, advantages, and suggestions for IoT-based smart homes. Challenges are identified in terms of communication technology in smart homes. Various suggestions are provided to use these communication components. Users must use these components to read the instructions for handling them carefully. Handling these components carefully leads to efficient energy saving, safety, security, and reliability to control communication devices with the best user experiences.

The challenges identified [12] in implementing a smart home-based automation system are detecting human motion and storing it in a cloud for surveillance purposes. Introducing weather prediction and energy conservation modules and adding more communication methods as a backup if one communication system fails to access the internet are a few other challenges.

For the reader's convenience, we have listed some of the major challenges discussed above in the implementation of IoT-based smart home systems based on the review.

- Human Motion Detection
- Security and Privacy
- Scalability
- Lack of Global Standards
- Interoperability
- Device Connectivity
- Affordable Cost

4 Conclusion

A recent trend has emerged in IoT-based smart home applications in the past few years. Enlighten the importance of its applications is important in this field. Much research is trending in this field, although some of the challenges remain exists. This article aims to analyze various applications and challenges in the development of IoT-based smart home environments. We found that most of the applications are based on home security and providing energy-efficient and cost-effective solutions. We found the research gap in terms of developing the communication standards for diverse devices. Many researchers have identified security and privacy as a major challenge in most IoT-based smart home applications. However, other challenges are identified in terms of human motion detection, scalability, lack of global standards, interoperability, data processing and management, mobility management, resilient architecture, device connectivity, and affordable cost. Simultaneously, the various approaches like selecting suitable sensor devices, reducing energy consumption, and awareness of security threats and attacks can solve most of the challenges in smart IoT-based home systems and open new opportunities in the research arena. New evolving technologies like blockchain, fog and edge computing, deep learning can be utilized to solve most of these challenges. At present, research has yet to discover more IoT-based applications for smart home automation and energy-efficient approaches. Future research should adopt more interdisciplinary and innovative approaches to discover the solutions for the identified challenges in the literature.

References:

[1] O. Galinina, K. Mikhaylov, S. Andreev, A. Turlikov and Y. Koucheryavy, "Smart home gateway system over Bluetooth low energy with wireless energy transfer capability," *Eurasip Journal on Wireless Communications and Networking*, vol. 178, no. 18, pp. 1-18, 2015.

[2] S. Marksteiner, V. J. E. Jiménez, H. Valiant and H. Zeiner, "An overview of wireless IoT protocol security in the smart home domain," in *IEEE International Conference on Internet of Things Business Models, Users, and Networks*, Copenhagen, Denmark, pp. 1-8, 2017.

[3] T. Malche and P. Maheshwary, "Internet of things (IoT) for building smart home system," in *International Conference on IoT in Social*, *Mobile, Analytics and Cloud,* Palladam, India, pp. 65-70, 2017.

[4] M. Tao, J. Zuo, Z. Liu, A. Castiglione and F. Palmieri, "Multilayer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Generation Computer Systems*, vol. 78, no. 3, pp. 1040-1051, 2018.

[5] S. Pirbhulal, H. Zhang, E. Alahi, M. Eshrat, H. Ghayvat *et al.*, "A novel secure IoT-based smart home automation system using a wireless sensor network," *Sensors*, vol. 17, no. 1, pp. 1-69, 2017.

[6] A. R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta and M. AliKarar, "A smart home energy management system using IoT and big data analytics approach," *IEEE Transactions on Consumer Electronics*, vol. 63, no. 4, pp. 426-434, 2017.

[7] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, pp. 1-44, 2016.

[8] M. Chen, J. Yang, X. Zhu, X. Wang, M. Liu *et al.*, "Smart home 2.0: innovative smart home system powered by botanical IoT and emotion detection," *Mobile Networks and Applications*, vol. 22, no. 6, pp. 1159-1169, 2017.

[9] J. KimKim, "HEMS (home energy management system) base on the IoT smart home," *Contemporary Engineering Sciences*, vol. 9, no. 1, pp. 21-28, 2016.

[10] S. Anwar and D. Kishore, "IoT based smart home security system with alert and door access control using smart phone," *International Journal of Engineering Research & Technology*, vol. 5, no. 12, pp. 1-5, 2016.

[11] S. W. Kum, M. Kang and J. I. Park, "IoT delegate: smart home framework for heterogeneous IoT service collaboration," *Korean Society for Internet Information Transactions on Internet & Information Systems*, vol. 10, no. 8, pp. 3958-3971, 2016.

[12] V. Govindraj, M. Sathiyanarayanan and B. Abubakar, "Customary homes to smart homes using internet of things (IoT) and mobile application," in *International Conference on Smart Technologies for Smart Nation*, Bengaluru, India, pp. 1059-1063, 2017.

[13] M. Al-Kuwari, A. Ramadan, Y. Ismael, L. Al-Sughair, A. Gastli *et al.*, "Smart-home automation using IoT-based sensing and monitoring platform," in *IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering,* Doha, Qatar, pp. 1-6, 2018.

[14] F. Saeed, A. Paul, A. Rehman, W. H. Hong and H. Seo, "IoT-based intelligent modeling of smart home environment for fire prevention and safety," *Journal of Sensor and Actuator Networks*, vol. 7, no. 1, pp. 1-11, 2018.

[15] Z. Shouran, A. Ashari and T. Priyambodo, "Internet of things (IoT) of smart home: privacy and security," *International Journal of Computer Applications*, vol. 182, no. 39, pp. 3-8, 2019.

[16] Y. Yao, J. R. Basdeo, O. R. Mcdonough and Y. Wang, "Privacy perceptions and designs of bystanders in smart homes," in *Proc. of the ACM on Human-Computer Interaction*, pp. 1-24, 2019.

[17] C. Lin, D. He, N. Kumar, X.Huang, P. Vijayakumar *et al.*, "Homechain: a blockchain-based secure mutual authentication system for smart homes," *IEEE Internet of Things Journal*, vol. 7*,* no. 2, pp. 818-829, 2019.

[18] M. Tao, J. Zuo, Z. Liu, A. Castiglione and F. Palmieri, "Multilayer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Generation Computer Systems*, vol. 78, no. 1, pp. 1040-1051, 2018.

[19] Y. Ren, Y. Leng, J. Qi, P. K. Sharma, J. Wang *et al.*, "Multiple cloud storage mechanism based on blockchain in smart homes," *Future Generation Computer Systems*, vol. 115, no. 1, pp. 304-313, 2021.

[20] A. Jalal, M. A. Quaid and M. A. Sidduqi, "A Triaxial acceleration-based human motion detection for ambient smart home system," in *16th International Bhurban Conference on Applied Sciences and Technology,* Islamabad Pakistan, pp. 353-358, 2019.

[21] A. Jalal, M. A. K. Quaid and K. Kim, "A wrist worn acceleration based human motion analysis and classification for ambient smart home system," *Journal of Electrical Engineering & Technology*, vol. 14*,* no. 4, pp. 1733-1739, 2019.

[22] S. B. ud din Tahir, A. Jalal and M. Batool, "Wearable sensors for activity analysis using smo-based random forest over smart home and sports datasets," in *3rd International Conference on Advancements in Computational Sciences*, Lahore, Pakistan*,* pp. 1-6, 2020.

[23] J. Ding and Y. Wang, "A WiFi-based smart home fall detection system using recurrent neural network," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 4, pp. 308-317, 2020.

[24] G. Marques and R. Pitarma, "Enabling smart homes through health informatics and internet of things for enhanced living environments," in *World Conference on Information Systems and Technologies*, Terceira Island, Portugal, pp. 76-85, 2020.

[25] J. H. Park, M. M. Salim, J. H. Jo, J. C. S. Sicato, S. Rathore *et al.*, "CIoT-Net: a scalable cognitive IoT based smart city network architecture," *Human-centric Computing and Information Sciences*, vol. 9, no. 1, pp. 1-20, 2019.

[26] C. S. Nandyala and H. K. Kim, "From cloud to fog and IoT-based real-time u-healthcare monitoring for smart homes and hospitals," *International Journal of Smart Home*, vol. 10, no. 2, pp. 187-196, 2016.

[27] J. M. Batalla and F. Gonciarz, "Deployment of smart home management system at the edge: mechanisms and protocols," *Neural Computing and Applications*, vol. 31, no. 5, pp. 1301-1315, 2019.
[28] C. H. Lo and N. Ansari, "The progressive smart grid system from both power and communications aspects," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 3, pp. 799-821, 2011.
[29] M. Noura, M. Atiquzzaman and M. Gaedke, "Interoperability in internet of things: taxonomies and open challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796-809, 2019.
[30] M. O. Farooq, I. Wheelock and D. Pesch, "IoT-connect: an interoperability framework for smart home communication protocols," *IEEE Consumer Electronics Magazine*, vol. 9, no. 1, pp. 22-29, 2019.
[31] R. Nawaratne, D. Alahakoon, D. De Silva, P. Chhetri and N.Chilamkurti, "Self-evolving intelligent algorithms for facilitating data interoperability in IoT environments," *Future Generation Computer Systems*, vol. 86, no. 1, pp. 421-432, 2018.
[32] M. Tao, J. Zuo, Z. Liu, A. Castiglione and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Generation Computer Systems*, vol. *78*, no. 3, pp. 1040-1051, 2018.
[33] M. Noura, M. Atiquzzaman and M. Gaedke, "Interoperability in internet of things: taxonomies and open challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796-809, 2019.
[34] D. Mocrii, Y. Chen and P. Musilek, "IoT-based smart homes: a review of system architecture, software, communications, privacy and security," *Internet of Things*, vol. 1, no. 1, pp. 81-98, 2018.
[35] J. Mocnej, A. Pekar, W. K. Seah, P. Papcun, E. Kajati *et al.*, "Quality-enabled decentralized IoT architecture with efficient resources utilization," *Robotics and Computer-Integrated Manufacturing*, vol. 67, no.1, pp. 102001, 2021.
[36] G. Hafeez, Z. Wadud, I. U. Khan, I. Khan, Z. Shafiq *et al.*, "Efficient energy management of IoT-enabled smart homes under price-based demand response program in smart grid," *Sensors*, vol. 20, no. 11, pp. 3155, 2020.
[37] S. K. A. Shah and W. Mahmood, "Smart home automation using IoT and its low-cost implementation," *International Journal of Engineering and Manufacturing*, vol. 10, no. 5, pp. 28-36, 2020.
[38] M. Collotta and G. Pau, "Bluetooth for internet of things: a fuzzy approach to improve power management in smart homes," *Computers and Electrical Engineering*, vol. 44, no. 1, pp. 137-152, 2015.
[39] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: challenges and solutions," *Journal of Cleaner Production*, vol. 140, no. 3, pp. 1454-1464, 2017.
[40] M. Alaa, A. Zaidan, B. B Zaidan, M. Talal and M. L. M. Kiah, "A review of smart home applications based on internet of things," *Journal of Network and Computer Applications*, vol. 97, no. 1, pp. 48-65, 2017.
[41] Y. Kim, Y. Park and J. Choi, "A study on the adoption of IoT smart home service: using value-based adoption model," *Total Quality Management and Business Excellence*, vol. 28, no. 9, pp. 1149-1165, 2017.
[42] S. Yoon, H. Park and H. S. Yoo, "Security issues on smart home in IoT environment," in *Computer Science and its Applications*, Berlin, Heidelberg: Springer, pp. 691-696, 2015. [Online]. Available: https://link.springer.com/book/10.1007/978-3-662-45402-2.
[43] M. Talal, A. A. Zaidan, B. B. Zaidan, A. S. Albahri, A. H. Alamoodi *et al.*, "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: multi-driven systematic review," *Journal of Medical Systems*, vol. 43, no. 3, pp. 1-42, 2019.
[44] D. Shin, V. Sharma, J. Kim, S. Kwon and I. You, "Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks," *IEEE Access*, vol. 5, no.1, pp. 11100-11117, 2017.
[45] A. A. Zaidan, B. B. Zaidan, M. Y. Qahtan, O. S. Albahri, A. S. Albahri *et al.*, "A survey on communication components for IoT-based technologies in smart homes," *Telecommunication Systems*, vol. 69, no. 1, pp. 1-25, 2018.
[46] Parameshwari, V., Sathishkumar, V.S., Premkumar, P., Srinevasan, M., "IoT enabled intelligent irrigation system for agriculture fields", *Journal of Advanced Research in Dynamical and Control Systems, Volume 11, Issue 8, Pages 269-279, 2019*
[47] Karthikeswaran D., Sudha V.M., Suresh V.M., Javed Sultan A., "A pattern based framework for privacy preservation through association rule mining", *IEEE-International Conference on Advances in Engineering, Science and Management, ICAESM-2012, Pages 816-821, March 2012.*