UPRIGHT PUBLICATIONS
https://upright.pub/index.php/ijrstp/

Original Contribution

Internet of Things (IoT) Technology for Use as Part of the Development of Smart Home Systems

Harshith Desamsetti[1]

Keywords: Frugal Labs IoT Platform (FLIP), Smart Home Systems, Remote Home, Home Automation System, Automated Home, Internet of Things (IoT)

International Journal of Reciprocal Symmetry and Theoretical Physics

Vol. 5, Issue 1, 2018 [Pages 14-21]

The Internet of Things (IoT) is a relatively new technology gradually advancing our world. With the Internet of Things, it is possible to conceive of a connected world. One example is a "Smart Home" built on the Internet. In a Smart household environment enabled by IoT, various objects, including lighting, household appliances, laptops, security cameras, and so on, are all connected to the Internet. This allows the user to monitor and control things regardless of the time or location in which they are located. This paper provides an overview of the Frugal Labs IoT Platform (FLIP), which may be used to construct smart homes that IoT enables. This paper explains the FLIP architecture and analyzes the functionalities of Smart Homes as well as the applications of Smart Homes. Finally, this paper proposes a system for implementing Smart Home services utilizing FLIP. The proposed method provided in this study is used to monitor and control the atmosphere of a smart home.

INTRODUCTION

Smart homes communicate with IoT-based digital gadgets to benefit users. In an ideal connected future, all smart home devices interact easily. IoT-based smart home technology has connected everyone at any time and place, changing life. Recent home automation systems are more advanced. These platforms enable all appliance data and service exchange. A smart home is a realm of IoT, the network of physical devices allowing electronic, sensor, software, and network connectivity. Smart homes have equipment to detect and control air conditioning, heating, ventilation, lighting, hardware, and security. Some term current systems with switches and sensors that connect with a central axis are "gateways." IoT manages network connectivity for these "gateways"—control systems with a tablet, phone, or computer user interface.

Several methods have been used to study IoT-based smart home applications since 2010. Research articles address the obstacles to smart home IoT application use in all categories and offer solutions. Research on smart home applications is varied. This survey seeks to illuminate technology ecosystems and help researchers understand their possibilities and gaps. It attempts to illuminate researchers' responses to new and disruptive technology, map the research landscape into a cohesive taxonomy, and identify the characteristics of this developing smart home technology research line. IoT and smart home applications are discussed (Suryaprakash et al., 2017).

The Internet has revolutionized human life by making it possible to communicate with anybody anytime and anywhere. Because of the tremendous advances that have been made in technology, many components, including sensors, processors, transmitters, and receivers, are now

[1]Department of Computer Science, Northern Illinois University, IL 60115, USA [harshithdesamsetti9@gmail.com]

readily available at a very affordable price. Therefore, each of these things has a place in the routine activities of our lives. If someone is interested in expanding the Internet's services, they should consider the Internet of Things as an expansion of those services. The Internet of Things (IoT) is becoming an increasingly important part of the modern Internet (Desamsetti & Mandapuram, 2017).

Internet-of-Things: The Internet, where the now active Internet network will connect to the computer systems that will connect to the physical items or things of the physical world. Things can be anything from furniture, kitchen equipment, electronic gadgets, or even cars. When these items link to the Internet in specified infrastructure using established protocols, the entire system is called part of the Internet of Things (IoT).

Things: Whether objects are real or virtual, whether they move or remain still, they will still be active participants in the system. Communication between different things is referred to as "things-to-things communication." If items can communicate or interact with humans in the future, we shall refer to this type of communication as "things-to-human communication." Nevertheless, the Internet of Things is more than just a far-reaching concept for the future. It is already here and affecting various things, not only the advancement of technology. These things and communicating devices, previously used to communicate with the Internet, can set themselves independently and function without a human operator's assistance.

Smart Home: A home or other living environment equipped with technology that enables all household equipment and appliances to be managed automatically and may be controlled remotely is referred to as a "smart home." Through the use of the Internet, users of smart homes are given the ability to effortlessly monitor and control all of the equipment and appliances in their houses. The network architecture that home appliances connect to is predefined and proper, and they use standard protocols. The fundamental concept of Internet of Things-based smart homes is illustrated in (Biljana et al., 2017). The entirety of the system may be broken down into two distinct sections: the first section has all of the home devices, switch modules, and RF transmitter-receivers; the second section contains all of the interface devices, CPU, data collector, and GPRS module components that will communicate with the Internet. Only four domestic devices—a light, a fan, a television, and a gas outlet—have been displayed for our perusal and evaluation in this paper. However, in practice, a user can connect several devices at once. The switch modules will allow connection to all of these everyday household gadgets.

Any module that can receive a signal and change its state in response to that signal can be contained within a switch module. The switch module is attached to the device so that if it changes forms, the household device to which it is connected will also change. The usage of relays as a switch module is possible. It is a device that uses electromagnetic forces and is often known as a relay switch. It keeps two electrical circuits separate while simultaneously connecting them magnetically. There are three different contactors in a simple relay. These contractors are designated as usually open (NO), normally closed (NC), and shared (COM). In most configurations, COM is linked to the NC. The relay is in the NO state when conditions are standard, and the device controlled by the relay is not operating in the working mode. When it detects a signal, it toggles the state to "not connected," and the apparatus returns to its functional state.

Switch modules will connect with the intelligent central controller using an RF transceiver. One transceiver will be built into each switch module, and combining all switch modules into a single transceiver will also be possible. Each switch module and device will bestow a unique identity to facilitate their recognition. A connection will be made for one RF transceiver at the intelligent central controller. The frequency of 433 MHz is used for communication between RF modules. The band at 433 MHZ has been set aside expressly for use in RF communication. The intelligent central controller will interface between the home devices and the internet server. There will not be a single piece of hardware serving as the smart central controller. It will be a collection of electronic components including, but not limited to, a microcontroller, CPLD processor, RF transceiver, GPRS or Zigbee module, etc. A microcontroller is versatile enough to be the primary controller and data processor. Since the microcontroller can easily capture data, this component can also serve as an interface device.

SMART HOUSES HISTORY

The first household appliances, including a vacuum cleaner, were developed in 1901, and the first vacuum cleaner was patented in 1907. After some

time, electric appliances such as dryers, freezers, irons, and others were developed. In 1966-1967, the ECHO IV was the first device to manage machines by turning them on and off and regulating the house's temperature. The 1970s saw the introduction of several security monitoring and lighting control devices. Most households in England had color televisions by the end of the 1980s, and by 1990, half of all English residents owned video recorders. In 1991, technology designed to assist older people was introduced.

In 1994, more individuals started using rotary dryers in addition to cordless house phones, DVD players, PlayStations, and multimedia PCs. In 1998, ISDN and the Internet were introduced with other new communication networks and peripherals, such as web television and video phones. The year 2000 saw the beginning of the rise in popularity of the "smart house," which was made possible by the availability of various technologies at prices that were within reach. 2002 Provide users of smart houses with the ability to operate their homes via remote control. 2005 marked the debut of the world's first wearable intelligent health system. 2009 saw the first cloud implementation as a component of the wise house system. In 2015, the human voice was used as a controller for smart homes (Li & Yu, 2011).

SECURITY IN SMART HOUSES

In a smart home, connected Internet of Things (IoT) devices transfer data collected by sensors across a wired or wireless transmission network, as depicted. The system must analyze data from many sensors without missing some data due to network congestion (Gutlapalli, 2016a). Additionally, it needs to ensure that suitable security measures are taken for transmitted data and prevent it from being interfered with or monitored from the outside. When some customers purchase Internet of Things devices for their homes, they frequently consider the device's performance and natural function more than the potential security risks they may face due to their purchase. On the other hand, Internet-connected gadgets and most of the equipment in smart homes need a standardized implementation environment and sufficient computer power dedicated to security (Gutlapalli, 2017a). As a result, the implementation of a complicated security system is challenging. A course of action. In the real world, the probability of someone entering our home if we accidentally leave the door open is relatively low. Will step inside, but in networks, there are an infinite number of persons who can check all the entries continuously. This portion of total security is discussed in each component of the smart home system: the Internet of Things, the user control system, and the network, both a layer and a cloud of different things.

IOT DEVICES

A smart home includes two distinct collections of Internet of Things devices. The gadgets that require communication in both directions comprise the first device category (Alaa et al., 2017). The second category includes home products with a single-way connection, such as a smart TV, lighting system, and charger. Solar panels are an example of the first group because they require bi-directional communications to give the utility company power that is not essential, and the alternating current is expected to receive a signal from the utility provider to limit the amount of power density (Gutlapalli, 2016b). On the other hand, the second group only needs a single link to relay the data on electricity consumption. The capabilities of the devices in the second group about resources are greater than those in the first group (Mandapuram, 2016).

IOT DEVICES THREAD AND SECURITY

Its owners can be confronted with various problems, difficulties, and risks. One of the researchers brought up the point. Those relating to the safety and confidentiality of the devices being utilized constitute one of the most significant of these difficulties. Most people who use Internet of Things devices need to be made aware of the necessary IoT security architecture, which prevents them from dealing with the privacy and safety concerns raised by the Internet of Things (Lal & Ballamudi, 2017). Devices connected to the Internet of Things are among the most common targets, and some types of electronic attacks aim to obtain access to users' personal information because of the relative ease of data transmission between these intelligent gadgets. Many Internet of Things devices are vulnerable to attack or penetration because of weak passwords and may not have sufficient security measures where they are used. Hewlett-Packard Development Company estimates that around 70% of the most widely used Internet of Things devices have already been penetrated, and most IoT devices collect data as a single unit. Recognized on an individual level. For instance, in the case of a DDOS assault (Yan et al.,

2014), the events that took place in two buildings, Lappeenranta and November of 2016 Finland, most of the automated systems controlled by thermostats and other devices stopped. Since testing has been done on distribution, ventilation, and the provision of hot water, the heating devices have been out of commission for more than a week due to these attacks that are removing people's sources of comfort, putting individuals in danger, and destroying infrastructure (Gutlapalli, 2017b).

It is one of the most critical legal difficulties that should not be ignored that data privacy, access to its management, and security pose. Need to remember about. There are many legal concerns around the privacy of data and its preservation, both of which include sensitive information (Desamsetti, 2016a). Concerning the user of specific devices. Therefore, it is necessary to decide who has the authority to access, display, and safeguard the data, whether it be an audio tape, a video recording, or another technology; it is essential to keep it out of the wrong hands to avoid it from being misused.

Because these devices store some of the most vital information hackers seek, they will become one of the most critical targets. Principal factors that provide cybercriminals access to them and allow them to embed their dangerous programs within them for several years' factors, the most significant of which are as follows:

- The ease with which smart devices, like cell phones in general, can be disseminated and acquired worldwide.
- Most intelligent gadgets that are commonly used run on an open platform, making it easier for hackers to attack the devices' vulnerabilities.
- A total need for awareness of the dangers and problems associated with using these technologies.

USER CONTROL DEVICE

An intelligent house smartphone system is not limited to control alone; it can also be used for data exchange and fulfilling user requirements. The user's life is made more accessible by using this type of system, but as a result, there are concerns with the system's security (Gaikwad, 2015).

- Problems with the power supply or the Internet If there is an issue with the device's ability to connect to the Internet or with the device's power supply, this results in a loss of connection between the owner and the house gadget.
- A problem with the software: The fact that the intelligent house smartphone system has a flaw in its software implementation makes it an attractive target for an attacker.
- Leakage of Confidential Data: The loss of information and leakage of data in the network may occur when the computer is either not secure or does not have data encryption.
- Denial of service (DoS): if a DoS attack is launched against the smart home system, it will block the user from accessing the control panel.

Eavesdropping attack: This exploit allows hackers to acquire a username and password when the user authenticates his access in a mobile app by listening in on the conversation between the user and the app.

NETWORK LAYERS

Generally, a Home Area Network (HAN) has two different modes of communication with Internet of Things devices. One method uses intelligent meters to network operation centers and other actors as the interface. Using a separate control and aggregation node is yet another method that can be used to interact with WAN and NAN networks directly. The smart meter (SM) is connected to the AMI innovative network, which is placed in the communication network infrastructure between devices on the HAN (Gutlapalli, 2017c). This is how all communications within the Bright House are made: through the AMI innovative network. Within this section, we will present a concise summary of the many attacks that can be made against wireless networks (Ghayvat et al., 2015).

Attacks using RFID: Radio frequency identification in intelligent environments enables control and differentiation of each object and storage of device identity data. However, there are some security flaws with RFID Attacks on RFID Tags: Cloning and spoofing attacks pose a significant risk to the information on RFID tags. These attacks can be devastating. This attack aims to produce an almost identical replica of the RFID tags. Eavesdropping attacks on RFID Readers are regarded as an assault against RFID Readers (Dekkati & Thaduri,

2017). Listening in on the RFID reader and stealing confidential information from the tags is a bad idea.

Attacks on WSNs: The Wireless Sensors Network (WSN) is a wireless connection of distinct nodes that are comprised of sensors. This network has a restricted bandwidth. The primary mode of communication in these networks is established between the base station and the sensor. It has the potential to strike by the bogus Routing Attack: In this type of attack, the attacker transmits fake route information to disrupt a communication that is going smoothly. Unfairness Attacks: This type of attack involves a rogue node that broadcasts a noise signal to generate collisions in the data transfer between nodes and depletes the network's resources (Chong et al., 2011).

WPA (WiFi Protected Access) is a protection system for wireless local area networks developed by the WiFi Business Alliance based on IEEE 802.11i. Access control and encryption are the two aspects of WiFi security that are most crucial to address. The WEP relies on the first-generation authentication technique for WiFi, which is insecure.

Bluetooth is a collection of protocols and functions encased in a stack. It possesses low transmission power and has a limited range. Most attacks on Bluetooth are brought about by users who do not change the pre-configured settings on their devices (Ballamudi & Desamsetti, 2017). A possible vulnerability in Bluetooth. A Denial of Service Attack could occur because Bluetooth can only manage a limited quantity of data at once. The attacker can exploit this vulnerability by having them submit a significant number of pairing request packets. This inhibits a valid user from connecting their device, which could result in the loss of battery life or unusable. Replay Attack: an attacker can transmit a reply attack with just one line of code by including the data it wishes to deliver in a capture file.

SYSTEMS USED IN BRIGHT HOUSE

Smart home systems suffer from various drawbacks, the most common of which are the high running costs of their many components, the limited ability of users to remotely monitor their properties, and inadequate levels of system security. The researchers who worked on them presented many different solutions to these difficulties. This section discusses five of the potential organizational structures. A Smart Home System that Integrates Blockchain Technology with the Internet of Things On the other hand, the proliferation of Internet of Things (IoT) devices and the use of these devices in smart homes have led to increased security threats. This is because most companies who manufacture IoT devices do not consider security protocols during production, which makes it simpler for malicious actors to compromise these devices (Desamsetti, 2016b). For instance, the most infamous malware assault, which goes by the name Mirai and is caused by manufacturers' default usernames and passwords, has resulted in 70.2% of consumers expressing major worries over their privacy and security. The researchers of this paper in Saudi Arabia conducted interviews with 270 people who are savvy homeowners. They were randomly selected to know the problems they face when they use IoT devices in the Bright House, and the result was that 72.2% of them do not trust the cloud, and 41.1% of them have no awareness of how their sensitive information is managed and stored in the cloud. They concluded that most problems lie with security, privacy, and dependability. Because smart houses need a system through which they can manage and monitor smart devices to meet security requirements, previous researchers proposed a solution: a mechanism by which a secure, easy-to-maintain, and cost-effective system for intelligent houses is designed through merging IoT devices with (BC) technology systems. A blockchain is a series of blocks connected by a previous hash. The blockchain is a distributed open ledger in which all network members may view each other's records (Lal & Ballamudi, 2017). The Internet of Things is represented by three different gadgets in the intelligent house scenario given by the researchers in this study.

Internet of Things (IoT) light and door security camera (Lal, 2015). This system fulfills the requirements for authentication through the utilization of a digital signature algorithm (DSA), confidentiality through the application of asymmetric cryptography, integrity through the utilization of a hash method, and availability (Mandapuram, 2017a).

BENEFITS AND CHALLENGES OF IOT AT HOME

The Internet of Things's primary objective is to connect devices to a network at any time and location. There is a wide variety of smart home

technology, ranging from smart toothbrushes to smart refrigerators. Internet of Things technologies are used in home automation and security systems, wearable devices, and personal health systems. According to Wang et al.'s research, some perceived benefits of smart home gadgets include "performance expectancy, effort expectancy, compatibility, and image" (Thaduri et al., 2016). As a result, people anticipate that smart home gadgets will enhance their activities around the house and simplify any operational challenges they face. In addition to this, the user's lifestyle is taken into consideration when designing an intelligent home. An additional benefit is the image, which visually represents the user's condition. It adds prestige to one's life to call one's home a smart home and employ innovative technology regularly (Bing et al., 2011).

The Internet of Things at home presents several severe concerns despite its many advantages. the most significant hazards associated with smart homes include "privacy, security, performance, time, and financial risks." Because the services for smart homes are delivered over a wireless network, there is also the possibility of unauthorized individuals gaining access to the system. This presents a potential security risk. The limited processing capabilities of Internet of Things (IoT)-powered smart homes render them susceptible to security and privacy risks, even though these houses address a wide range of social concerns and provide users with innovative, one-of-a-kind services (Lal, 2016). The Internet of Things can be risky for users since manufacturers and consumers of smart devices worry significantly more about the functionality and cost of those devices than they do about the devices' privacy and security. Each additional piece of hardware a user adds to their smart home opens the possibility of being hacked and stealing their information (Mandapuram, 2017b). A significant number of gadgets that are connected to the Internet need to be more secure.

It is vital to mention that users of Internet of Things technologies, as well as public and private infrastructure, including the infrastructure of the Internet, are put in danger, and one of the benefits of smart homes is access to the Internet anywhere and at any time. However, this benefit may also create significant threats, such as the possibility of hostile assaults and the theft of personal information. Using the Internet of Things poses certain privacy leakage risks because the user's sensitive data is uploaded to a remote cloud. For example, it is required to establish a minimum security criterion before utilizing the device, such as a strong password. Additionally, it is necessary to have the capacity to automate the update process if even the slightest threat is discovered, suggesting that to maintain security, the password should be checked frequently and changed after a predetermined amount of time has passed. This prevents unauthorized individuals from accessing the system through private accounts. Protecting the WiFi network and establishing a secure connection are two more recommendations. Following these steps will prevent unauthenticated users from connecting to the system. To summarize, the solution to the challenges caused by the IoT is to ensure that the devices have a high level of security (Malche & Maheshwary, 2017).

The Smart Home system has the potential for various concerns, problems, and significant hurdles. Because the number of IoT apps is increasing, managing all of these applications in an IoT environment can be challenging. It is a challenge that comes up how to manage and regulate all these different apps that are increasing. If these ever-growing applications were not controlled effectively and conveniently, the entire system could not be more pleasant or secure. On the server side, there is no particular technique for authenticating users. Hence, the level of security could be higher. This could eventually lead to the system becoming vulnerable (Thodupunori & Gutlapalli, 2018)). If an attacker accessed a victim's home, they could turn off the victim's entire smart home system. Connectivity is another potential issue. Another area for improvement is determining how to maintain connectivity at all times and at any location. 3G services are utilized for communication that is directed toward the Internet. However, there is a possibility that it has signal issues, which means that it might only connect sometimes. The Internet of Things environment calls for the operation of the smart home system to take place in real-time. The frequency of 433MHz is utilized for radio frequency identification. This may lead to interference issues.

CONCLUSION

The Internet of Things has transformed life. IoT automates domestic duties, keeps people secure, and saves energy in the high-tech smart home. IoT-enabled smart gadgets may detect activity, collect data, and tailor user experiences. Despite its benefits, the IoT's growth and development pose a security risk. Since all smart devices are

Internet-connected, cyberattacks and hacks are increasing. Despite safety concerns, the IoT continues to evolve. IoT now refers to the many physical devices connected to the Internet to gather, analyze, and process massive volumes of data. Internet objects may soon be present in all fields and businesses, allowing connected equipment to exchange information without human involvement.

REFERENCES

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, *97*, 48-65. https://doi.org/10.1016/j.jnca.2017.08.017.

Ballamudi, V. K. R., & Desamsetti, H. (2017). Security and Privacy in Cloud Computing: Challenges and Opportunities. *American Journal of Trade and Policy*, *4*(3), 129–136. https://doi.org/10.18034/ajtp.v4i3.667

Biljana, L., Stojkoska, R., Kire, V. T. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production, 140*(3), 1454-1464. https://doi.org/10.1016/j.jclepro.2016.10.006.

Bing, K., Fu, L., Zhuo, Y., Yanlei, L. (2011). Design of an Internet of Things-based smart home system. *2nd International Conference on Intelligent Control and Information Processing, 2011*, 921-924. https://doi.org/10.1109/ICICIP.2011.6008384.

Chong, G., Zhihao, L., Yifeng, Y. (2011). The research and implementation of smart home systems based on the Internet of Things. *International Conference on Electronics, Communications and Control (ICECC), Ningbo*, *2011*, 2944-2947. https://doi.org/10.1109/ICECC.2011.6066672.

Dekkati, S., & Thaduri, U. R. (2017). Innovative Method for the Prediction of Software Defects Based on Class Imbalance Datasets. *Technology & Management Review*, *2*, 1–5. Retrieved from https://upright.pub/index.php/tmr/article/view/78

Desamsetti, H. (2016a). A Fused Homomorphic Encryption Technique to Increase Secure Data Storage in Cloud Based Systems. *The International Journal of Science & Technoledge*, *4*(10), 151-155.

Desamsetti, H. (2016b). Issues with the Cloud Computing Technology. *International Research Journal of Engineering and Technology (IRJET), 3*(5), 321-323.

Desamsetti, H., & Mandapuram, M. (2017). A Review of Meta-Model Designed for the Model-Based Testing Technique. *Engineering International*, *5*(2), 107–110. https://doi.org/10.18034/ei.v5i2.661

Gaikwad, P. P., Gabhane, J. P., Golait, S. S. (2015). A survey based on smart homes system using Internet-of-Things. *International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), 2015*, 0330-0335. https://doi.org/10.1109/ICCPEIC.2015.7259486.

Ghayvat, H., Mukhopadhyay, S., Gui, X., Suryadevara, N. (2015). WSN- and IOT-Based smart homes and their extension to smart buildings. *Sensors*, *15*(5), 10350-10379. https://doi.org/10.3390/s150510350

Gutlapalli, S. S. (2016a). An Examination of Nanotechnology's Role as an Integral Part of Electronics. *ABC Research Alert*, *4*(3), 21–27. https://doi.org/10.18034/ra.v4i3.651

Gutlapalli, S. S. (2016b). Commercial Applications of Blockchain and Distributed Ledger Technology. *Engineering International*, *4*(2), 89–94. https://doi.org/10.18034/ei.v4i2.653

Gutlapalli, S. S. (2017a). Analysis of Multimodal Data Using Deep Learning and Machine Learning. *Asian Journal of Humanity, Art and Literature*, *4*(2), 171–176. https://doi.org/10.18034/ajhal.v4i2.658

Gutlapalli, S. S. (2017b). The Role of Deep Learning in the Fourth Industrial Revolution: A Digital Transformation Approach. *Asian Accounting and Auditing Advancement, 8*(1), 52–56. Retrieved from https://4ajournal.com/article/view/77

Gutlapalli, S. S. (2017c). An Early Cautionary Scan of the Security Risks of the Internet of Things. *Asian Journal of Applied Science and Engineering*, *6*, 163–168. Retrieved from https://ajase.net/article/view/14

Lal, K. (2015). How Does Cloud Infrastructure Work?. *Asia Pacific Journal of Energy and Environment*, *2*(2), 61-64. https://doi.org/10.18034/apjee.v2i2.697

Lal, K. (2016). Impact of Multi-Cloud Infrastructure on Business Organizations to Use Cloud Platforms to Fulfill Their Cloud Needs. *American Journal of Trade and Policy*, *3*(3), 121–126. https://doi.org/10.18034/ajtp.v3i3.663

Lal, K., & Ballamudi, V. K. R. (2017). Unlock Data's Full Potential with Segment: A Cloud Data Integration Approach. *Technology &Amp; Management Review*, *2*, 6–12. https://upright.pub/index.php/tmr/article/view/80

Lal, K., & Ballamudi, V. K. R. (2017). Unlock Data's Full Potential with Segment: A Cloud Data Integration Approach. *Technology & Management Review*, *2*(1), 6–12. https://upright.pub/index.php/tmr/article/view/80

Li, B., Yu, J. (2011). Research and application on the smart home based on component technologies and Internet of Things. *Procedia Engineering, 15*, 2087-2092. https://doi.org/10.1016/j.proeng.2011.08.390.

Malche, T., Maheshwary, P. (2017). Internet of Things (IoT) for building smart home systems. *International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC), 2017*, 65-70. https://doi.org/10.1109/I-SMAC.2017.8058258

Mandapuram, M. (2016). Applications of Blockchain and Distributed Ledger Technology (DLT) in Commercial Settings. *Asian Accounting and Auditing Advancement, 7*(1), 50–57. https://4ajournal.com/article/view/76

Mandapuram, M. (2017a). Application of Artificial Intelligence in Contemporary Business: An Analysis for Content Management System Optimization. *Asian Business Review*, *7*(3), 117–122. https://doi.org/10.18034/abr.v7i3.650

Mandapuram, M. (2017b). Security Risk Analysis of the Internet of Things: An Early Cautionary Scan. *ABC Research Alert*, *5*(3), 49–55. https://doi.org/10.18034/ra.v5i3.650

Suryaprakash, S., Mathankumar, M., Ramachandran, R. (2017). IOT based home automation system through adaptive decision making fuzzy algorithm. *Research Journal of Engineering and Technology,* 8(3), 268-272. https://doi.org/10.5958/2321-581X.2017.00045.9

Thaduri, U. R., Ballamudi, V. K. R., Dekkati, S., & Mandapuram, M. (2016). Making the Cloud Adoption Decisions: Gaining Advantages from Taking an Integrated Approach. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *3*, 11–16. https://upright.pub/index.php/ijrstp/article/view/77

Thodupunori, S. R., & Gutlapalli, S. S. (2018). Overview of LeOra Software: A Statistical Tool for Decision Makers. *Technology & Management Review, 3*(1), 7–11.

Yan, Y., ZhiFang, X., Zhu, X. (2014). A middleware of IoT-Based smart home based on service. *Applied Mechanics and Materials*, *507*, 182-186. https://doi.org/10.4028/www.scientific.net/AMM.507.182

--0--