REVIEW ON IOT BASED SMART HOME SYSTEM

Dr. Pradeep V[1], Nisarga Naik[2], Nandini Boragave[3], Nikita Shetty[4], Navya Y R[5]

Department of Information Science and Engineering[1-5]

Alva's Institute of Engineering and Technology, Mijar, Karnataka,India

ABSTRACT

The Internet of Things (IoT), a giant network of devices, all connected to the internet and be identified by its IP address. A classic example of IoT at work is found in the smart home where you can check and control the performance of such household appliances. This requirement opens up the market for more advanced security options designed to meet IoT systems. Most of the security issues come down to authorization & authentication. In the worst case, infringement of security breaches like Cyber-attack where a possible unauthorized control which changes sensors and actuators opening doors for burglar to have access. This paper proposes an extra security layer by introducing the multi-factor Authentication to reduce challenges unauthorized access. We discuss a number of these factors, including advances in facial recognition—once deemed impossible given the plethora of biometric data collected by cameras on most modern computers and smartphones. In this paper, we have analyzed what are the limitations of existing IoT smart home systems and how these can be improved by introducing (i) required system modules in our proposed architecture along with (ii) a better user registration process as well as login authentication scheme. The objective of this technical report is to describe how we are experimenting with the mobile health system based on dynamical systems and software architecture as solutions. Though unwittingly naive, we have begun to develop a smart home management software architecture for IoT through literature review from selected articles around the web that had showed many aspects but non of them has include any facial recognition and liveness detection in their proposed solutions.

KEYWORD*:-IoT, includes smart home systems, new architectural solutions and use of RFID for security upgrade.*

1.INTRODUCTION

Certain devices, or even entire systems of such connected gadgets can be controlled by looking up certain platforms Smart home – a modern approach Home automation (also known as domotics) refers to newly built smart homes that have been constructed using groundbreaking technological advancements. For example with Apple HomeKit you can add your products and accessories to the home app on iOS devices such as iPhone, apple watch. It can be accomplished via a custom app or by utilizing iOS native applications like Siri. Take Lenovo's Smart Home Essentials, a trio of smart home items that can be managed by means of Apple's HomeKit or Siri however you don't require a Wi-Fi organize. Smart home for the internet of things is a main aim in this paper and research, as it includes

Internet-of-Things: The Internet of Things (IoT) is the network which provides connectivity between common internet infrastructure to real-world physical objects/"things". These objects can consist of a broad range like home appliances, devices, vehicles etc. The all things that it connects to the internet using a defined standard protocol and infrastructure, are called living at hi-secure environment through using many devices; sensors & controllers..... etc.

Objects: The objects can either be physical or virtual, mobile or stationary and they are the things that actually involve in all kind of system. This sort of interaction is called Things To things/ devices/devices communication. IOT when the same things communicate or interact with humans also termed as Things-to-Human Communication. But the Internet of Things is not just a vision for tomorrows — it exists now and looks beyond technological innovation. These are the communicating objects that connect you to internet of things, which have their own configurations and capable of functioning without human intervention.

Smart Home: A smart home is a living area with devices and system that can be automatically or remotely controlled for the convenience of its resident. Smart homes allow users to monitor and control their home from anywhere in the world by using smart devices through internet. Connected via a well-defined network architecture utilising standard protocols.

The whole system can integrate into two parts: part one containing all the home devices and switch modules with Information Science Engineering RF transmitter/ receiver; another part contains interface devices, processors, data collectors/GPRS Modules for internet communication. This paper mainly details 4 household devices: a light, a fan and TV along with main gas outlet. But in reality, users can and do connect more devices. The switch modules will be used to connect all the household appliances. The switch module can be any kind of a module that switching its state upon getting signal. The switch module hooks the same as a device, and if state changed from one of them it changes also at connected household. The simplest form of relay is the switch module in which are named as relay switches, and these relays can be used as a separate component for switching applications. They Electrically Separate Two Circuits but Physically Connect Them via Magnetism Three Main Contacts in a RelayA relay is depicted with its three principle contacts: Generally Open, for example NO; Normally Close, or NC; and COM (purpose of ordinary association). The computer is usually coupled to the NC over COM. In normal state, when household devices are OFF relay remains at NC state. When receives a signal, it shifts the equipment to NC state that turns on the apparatus. RF transceivers are used to connect Switch modules with the smart central controller. One switch module per transceiver, or a single transceiver connecting to multiple switch modules. The devices and each switch module will have an individual identity which is used to identify these. The smart central controller must have connection with one RF transceiver. RF Modules communicate each other with 433MHz frequency which is dedicated for RF communications. Smart Central System (SCS). It is the interface between all household devices and internet server. It will not be one device but a combination of devices — microcontroller, CPLD core, RF transceiver chipset and GPRS or Zigbee module. Because of this, the microcontroller may also serve as a main controller or processor: processing other data to be passed in and used later (e.g. another measurement) through that same interface device itself — which is then much simpler because it handles things like point-to-point communication/data acquisition; thus none can interfere into what should otherwise remain an input-only path with no shared state changeable by others than those who initiated any action precedding one from initiating themselves against some signal type accompanied due timing whatsoever!.

2. INTERNET OF THINGS FOR SMART HOME

Home automation, on the other hand, is a broader concept that includes applications such as lighting control or remote monitoring of an irrigation system.deepcopy Long-term advantages might include energy savings through automatic light and appliance switch off. Companies are investigating a long list of IoT uses — all falling into one of two general areas. The types of transportation systems identified in the initial group are those which have interconnected devices that automate and communicate as part of a system helping to improve day-to-day life for people. Basically, you can think of IoT as playing the role of TCC&R (track, command and control) here. Like, you can control room temp in a house and windows lighting electronic device with computer programming from your home or program to perform things automatically that we do regularly on manual bases. The Internet of Things is anticipated to have sustainable outcomes in terms of technology and futuristic system. As the characteristic feature of our modern information society, The architecture IoT integrates connection with things which may be unable to connect as well accountability and town combination or orchestrated emergence and measurable endeavors; To a internation treasury community at large provisioning extant & next internet — telecommunications-&-computational-stack for thing-to-be-connected. Though the term IoT has gained currency of late, connected devices on Internet are not a new bandwagon. A Trojan Room coffee pot was used as an early example of a network-connected appliance, one of the first in the world. Smart Home or Automated home can be created on such the platforms which control your smart devices and appliances. As an illustration, Apple HomeKit lets manufacturers provided that devices and accessories can interface with one another through the iPhone or Apple Watch. It will be possible to integrate this with a dedicated app, or through native iOS applications — eg Siri. An example is the Lenovo Smart Home Essentials, which are home automation devices that can be controlled with Apple's Home app or Siri without needing a WiFi connection. In this paper and in my research, the main idea is to give an overview for developing a smart home using Internet of Things security Specifically dealing with devices from Sensors — Controllers etc.

3. AIM and OBJECTIVE

This paper presents an IoT-based approach to home automation. Common applications include monitoring home conditions controlling home appliances, and managing home access through RFID cards and servo-controlled window locks [9]. However, this paper focuses on enhancing home security through IoT. Specifically, it deals with monitoring and controlling servo door locks, entry sensors, surveillance cameras, patrol vehicles, and smoke alarms, which help to ensure and improve home safety and security.

A user has access to the following features through a mobile app where they:

1. Can switch LED lights on or off and check their status.
2. Can lock and unlock doors using servo motors and check if the doors are locked or unlocked.
3. Can check if doors are closed or open using IR sensors.
4. Get an email alert if a door stays open for too long.
5. Receive a notification about who entered through the door as the camera takes a face picture and sends it to them by email.
6. Get an email alert if the fire detector senses smoke.
7. Can manage the surveillance vehicle to keep an eye on their residence.

This paper aims to provide a brief overview of IoT-based Smart Home Environments focusing on their groundbreaking technologies, areas of use, frameworks, and architectures. I don't intend to give a detailed explanation of each topic. Instead, my goal is to offer readers the basic principles and a quick rundown of each subject. I'll also include a bibliography for those who want to dig deeper into specific aspects of the topic.

3.1 Enabling Technologies for IoT

The ongoing improvements in information and communication technologies (ICT) combined with computer systems embedded frameworks and artificial intelligence have made the smart home vision a reality. By boosting traditional home automation systems with new capabilities smart homes can now showcase different forms of artificial intelligence. Smart home technology merges technology and services through home systems management to improve life quality. IoT Enabling Technologies: Radio Frequency Identification (RFID) Internet Protocol(EPC) Electronic Product Code Barcode Wi-Fi Bluetooth ZigBee Near Field Communication(NFC) Actuators Wireless Sensor Networks(WSN), AI

3.2. Application Areas of SHAS

The Internet of Things offers a flexible platform to support various applications. Its widespread use has led to many applications, including smart homes. The main Smart Home Automation System (SHAS) application areas are:

1. Environmental control: This includes traditional support for lighting/daylighting and Heating, Ventilation and Air Conditioning (HVAC) systems.
2. Monitoring and control
3. Health and safety
4. Telehealth care
5. Energy saving
6. Environmental control
7. Information access

Smart homes have different application areas:

- Smart homes for security
- Smart homes to care for the elderly
- Smart homes for healthcare
- Smart homes for childcare
- Smart homes for energy efficiency

- Smart homes for better living (music, entertainment, etc.)

3.3.Structure

A smart home is a house equipped with smart devices. A home network allows data exchange between devices and a residential gateway connects the smart home to the outside internet. Smart devices interact with residents or monitor them. , a home automation system has five key components.

3.4Devices under Control

These devices include all components such as home appliances or consumer electronics, that connect to and are controlled by the home automation system. Various connection technologies like WLAN, Bluetooth, Z-Wave interfaces, and others provide direct connectivity to the control network.

3.5 Sensors and Actuators

Sensors observe and monitor within the home system. They have an influence on a wide range of uses such as measuring temperature, humidity, light, liquid, and gas and detecting movement or sound. Actuators are the means by which the smart system can get things done. Mechanical actuators include pumps and electric motors, while electronic actuators include electric switches. IoT devices with sensors act as supervisors, and those with actuators act as performers. A system with both sensors and actuators will detect and act.

4.PROBLEMS AND CHALLENGES

The Smart Home system faces numerous problems and key challenges. As IoT applications grow , managing them all becomes tough. This raises questions about how to handle these growing applications . Without efficient and easy control of these increasing applications, the whole system might not be as comfortable or safe. Security is weak on the server side due to the lack of special authentication methods. This could make the system unsafe. An attacker might access a victim's home and break the entire Smart home system. Connectivity is another potential issue. Achieving connectivity anywhere anytime is also challenging. 3G services are used to connect to the internet. But signal problems might prevent constant connection. The Smart home system in an IoT setting should work in real time. RF identification uses 433MHz, which might cause interference problems.

Dhananjay Singh and others, along with Sarita Agrawal and colleagues, have highlighted several key challenges:

4.1 Standards: The IoT environment needs standardization as it grows worldwide. Questions arise about which standards to use how to ensure a secure medium, and how to make the system more reliable.

4.2 Identification: Each device requires a unique identifier to distinguish it from others.

4.3 Privacy: User data must remain confidential. Connections should protect privacy.

4.4 Authentication: Smart Home systems need authentication to guard against attackers. Servers should grant access to genuine users.

4.5 Security: The system should take proper steps against security threats. It should also reconfigure itself after attacks.

4.6 Integration: Integrating apps in an IoT setting poses the main challenge for IoT.

4.7 Coordination: linked objects, humans, programs, and processes need to coordinate.

4.8 Data Storage: The growing use of IoT leads to massive data collection. Finding storage for this huge amount of data presents a challenge. Large databases can address this issue. To get useful info from extra data, we need to use AI algorithms.

4.9 Network Self-Organization: The network's structure should allow every connected device to organize itself. In reality, the network itself should have the ability to self-organize.

5.CONCLUSION

Over the last few years smart homes using Internet of Things tech have popped up and grown alongside our fast-paced tech world. They give homeowners comfort and save them lots of time and effort. But they also bring new security issues. This paper looks at smart home security personal privacy, and weak spots bad guys could take advantage of. We checked out many earlier studies on this topic to break down the security risks smart homes face. We talk about what's been done with systems for running smart homes and compare different options. Many researchers have worked on building automated smart home systems with new tech to make homes more secure and private. This paper helps anyone who wants to set up a smart home pick a system that keeps them safe. It also gives researchers ideas to test out more smart home tech.

REFERENCES

[1] Gubbi , J. , Buyya , R. , Marusik , S. , & Palaniswamy , M. (2013). "Internet of Things (IoT): A Look at Infrastructure, and Future Directions." Future Generation Computing Systems 29(7), 1645-1660.

[2] Sicari S., Rizzardi A., Grieco, L. A., & Coen-Porisini A. (2015). "Security, Privacy, and Trust in the Internet of Things: A Way Forward." Computer Communications 76 146–164.

[3] Alrawais A. A., Hu, C., and Cheng, X. (2017). "Fog computing for the Internet: security and privacy concerns." IEEE Internet Computers 21 (2) 34-42.

[4] Mosenia, A., & Jha, N. K. (2017). "A thorough examination of Internet-of-Things security." IEEE Transactions on Emerging Topics in Computing 5(4) 586-602.

[5] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen (2017). "Security and Privacy in Smart City Applications: Challenges and Solutions." IEEE Communications Journal 55 (1) 122-129.

[6] Sicari S., Rizzardi A., Grieco, L. A., & Coen-Poricini A. (2015). "Security, Privacy, and Trust in the Internet of Things: A Way Forward." Computer Communications 76 146–164.

[7] Pereira , C. , Liu , C. ; H., and Jayawardene S. (2015). "The Technological Advancement of Internet Product Markets: A Survey." IEEE Transactions on Emerging Topics in Computing 3(4), 585-598.

[8] Mahalle, P. (1999). N. Relkar, P.S. N. , Shinde , G.N. , & Prasad , N.R. (2014) and the author. "Identity Management Framework for Internet of Things (IoT): Roadmap and Key Challenges." Journal of Computer Communication and Communication 2014 1-17.

[9] Roman R., Najera, P., & Lopez, J. (2011). "Security in the Internet of Things." Computers 44 (9) 51-58.

[10] Ammar M., Russell, G., & Crispo, B. (2018). "The Internet of Things: A Survey of IoT System Security." Journal Safety and Management, 38 8-27.

[11] Lee, I., and Lee, K. (2015). "Internet of Things (IoT): Services, investments and demanding situations for enterprise." Business Management fifty eight(4), 431-440.

[12] Sadeghi , A. R. , Waxman , C. , & Waidner , M. (2015). "Security and Privacy Challenges in the Business Internet." Proceedings of the 52nd Annual Design Automation Conference, 2015, 1-6.

[13] Zhang, Y., Zheng, J., & Hu, J. (2018). "A survey to examine security and privacy issues in smart grids." China Communications 15(2) 145-156.

[14] Chen, J., Zhang, Z., Hu, J., Li, Y., & Qin, J. (2018). "IoT-based smart rehabilitation system." IEEE Transactions on Industrial Informatics, 14(6), 2603-2612.

[15] Li S., Xu, L. D., & Zhao S. (2018). "The internet of things: a survey." Information Systems Frontiers 20(2) 243-259.

[16] Al-Fuqaha A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). "Internet of Things: A Survey of Enabling Technologies, Protocols, and Applications." IEEE Communications Research & Education 17(4), 2347-2376.

[17] Fernandes, E., Jung, J., and Prakash A. (2016). "Security Analysis of Emerging Smart Home Applications." Proceedings of the 2016 IEEE Conference on Security Privacy (SP), 2016 636-654.

[18] Haddadpajouh H., Dehghantanha, A., Khayami, R., and Cho, K. K. R. (2018). "A deep iterative neural network method to spot Internet of Things malware risks." Future Generation Computing Systems 85 88–96.

[19] Miorandi D., Sicari S., de Pellegrini, F., and Chlamtac, I. (2012). "The Internet of Things: Vision, Implementation, and Research Challenges." Ad hoc Communications 10(7), 1497–1516.d Actuator Networks, 6(3), 11