A Review on Autonomous Remote Security and Mobile Surveillance Using Internet of Things

Manoj Diwakar¹, Kanika Sharma², Ravi Dhaundiyal³, Sheetal Bawane³, Kapil Joshi¹, Prabhishek Singh⁶*

¹Department of CSE, Graphic Era deemed to be University, Dehradun, India
²Department of IT, IMS Noida, India
³,⁵Department of CSE, UIT, Uttaranchal University, Dehradun, India
⁴Department of ECE, Malwa Institute of Technology Indore, India
⁶Department of CSE, Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, India

*Corresponding author email: prabhishekSingh88@gmail.com

Abstract: From Generations, Security methods have always been improvised on the basis of modernisation of Technology. Now a day’s using man power for security have become less reliable as Humans can be manipulated using social/emotional hacking. Today most of the family members are employed and only the old aged members or toddlers of the family are left alone at home unattended and unguided. One of the best solutions to these problems is to use the things that are reliable and can’t be socially hacked. The primary aim that is achieved by this technology is to look after the unattended and other important activities. Problems like this can be handled by using IOT which involves Surveillance System, remote access, automated security systems, Cloud Computing and many more. Vast variety of problems can be solved by this technology. This can be used at personal level, organisational level or national level. This paper basically describes how Internet of things (i.e. Connecting multiple uncommon devices using internet and giving them instructions remotely as per required) can be used to achieve reliable high level security and can be used to make working simple and easy in some other important fields. IOT has limitless potential; it has the capacity to replace some previous technologies.

Keywords: Motile Surveillance, Remote Access, Automated Security Systems, IOT, Cloud Computing.

1. Introduction

Internet of things is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes that uses intelligent interfaces, have decision making capability and are efficiently and seamlessly integrated into information network. IOT [1] [2] has become hot topic in technology industry, policy, and engineering circle as this technology is embodied in a wide spectrum of networked products, sensors and network interconnections to offer new possibilities & capabilities that was not previously possible. At a large scale and industry level, implementation of IOT [2] promises to change, manipulate and transform many aspects of the way we live. IOT is a revolutionary, efficient and promising technology that represents the growing aspect of how people can connect to the internet in their social, personal and economic lives.

Overall, this paper has been written to provide a high level overview of the basics of IOT, how it helps in providing almost full-proof security and in other important aspects of our lives. This paper sheds light on IOT products like internet-enabled appliance, home automation components and energy management devices. IOT promises to be helpful, advantageous and worthwhile for people with disabilities and the elderly, enabling modified and improved levels of independence and quality of life. This paper helps the Internet Society Community to navigate and consider the promises and perils made by this technology. Some of the issues and challenges that this technology raises that need to be considered and addressed have been raised in this paper. This paper also acknowledges some of the unique aspects of internet of things that makes this a transformational technology of internet.
2. Working of Internet of Things Devices

IOT is the concept of basically connecting devices with Internet [1]. Devices includes cell phones, coffee makers, washing machines, fans, lamps and many other devices. Internet of things consists of all the web-enabled devices that collect, send and act on data they acquire from their surrounding environments using embedded sensors, processors and communication hardware. These connected smart devices can talk to other related devices and act on the information they get from one another. Cloud Networks plays a very significant role in acquiring all the data perceived by the devices which is further uploaded to the database of the cloud and are later retrieved with the help of server (physically located somewhere). All the devices trigger signals to the server and the server takes the actions that are saved in the memory or the server further signals the administrator to take the action accordingly [22-24].

The basic working of Internet of Things devices is shown below in Fig. 1.

![Fig. 1 Basic Working of Internet of Things Devices](image)

3. IoT Devices

The potential benefits of IOT are limitless and IOT devices are changing and transforming the way we work and live. The implementation of IOT [9] products is no longer a futuristic vision as there are already a number of products in the market that are working quite effectively and efficiently and also there are many other IOT [9] products that are under development process. To help clarify how the Internet of Things works, we’ve laid out some applications for the IOT, along with some specific devices.

Applications of the Internet of Things [9] with their products [2][3][4].

3.1 Smart Home

Smart homes are currently the most favoured and popular IOT application because it is the one that is easily and readily available and are affordable to consumers.

Product: Amazon Echo-Smart Home.- It works through a voice assistant which users can interact and talk to in order to perform numerous functions. This voice assistant is known as ALEXA (a Amazon product). Users can tell ALEXA to play music, call a cell phone number, tell the sports update, get weather report and many more.

3.2 Wearable

There are already a number of wearable products in the market that a person can use to perform and monitor simple day-to-day tasks. There are smart watches that are no longer just used for telling time. Implementation of smart watches has turned our wrists into a Smartphone holster by enabling text messaging, voice calling, health-monitoring and many more.

Product: FitBit One: This wearable device keeps the track of steps the user walked, floors the user climbed, calories he/she burned in a day, quality of sleep and many more. It also monitors the heartbeat rate and blood pressure. This device wirelessly synchronises with remote computers and Smart phones
through a cloud network in order to transfer your fitness data in user-understandable form (say charts) to monitor your progress.

3.3 Smart Cities

This application of IOT has the potential and power to transform an entire city by solving and proposing a set of solutions for the problems the citizens face each day. IOT can solve traffic congestion issues, pollution control, noise reduction etc.

Product: Barcelona: This Spanish city is foremost smart cities in the world after this city implemented various IOT products and initiatives that have helped in enhancing the functionality and smoothness of the city. Barcelona has smart environment due to the implement if IOT products.

3.4 Connected Car

Cars can be connected to each other through internet access and these connected cars can share these access with each other which in turn will help them to communicate with each other just like we connect wireless [12] [16] network in a home or office.

Product: AT&T - Connected Car: AT&T recently connected 1.3 million cars in mid of 2016 bringing total numbers of car it connects to 9.5 million. The car owners and the drivers don’t have to subscribe or pay for the connection.

3.5 Bot as a Medicine Dispenser

Healthcare of one’s family is of utmost importance. People tend to forget to take the medicine on time. Through this technology [5] we can keep a track of the users activities and informs the user whenever it is time to take the medicines. This technology uses a camera which always keeps the track of each family member by facial recognition and informs them of their uncompleted activities. If the medicines are not taken at the specified time then the Agent will directly send a message to the main user informing him that the certain family member have not taken the medicine [26].

This technology also overcomes the problem of the elderly to read the instructions and differentiate between the pills. Physical ailments can make opening medication containers difficult [6]. In this case the Agent will have inbuilt containers for each of the family members to dispense the required amount of medicines according to the prescription [27].

4. Intelligent House Security System

4.1 Introduction

Smart house[7] is an upcoming technology which has tremendous benefits, it can help a lot in saving precious resources by correcting common human mistakes like leaving the tap running, leaving the light, fans on or leaving the fridge door open etc. It eliminates the inconvenience caused after the owner loses the keys and deliberately reduces the burden of carrying a bunch of keys. There are lot more benefits of a smart house. But when it comes to security then there is still a great overhead in completely securing a smart house, below is a possible method which can be used to increase the security of smart houses.

4.2 Implementation

The smart house uses smart unlock [8][9] system for better security [10], i.e. by recognizing the owner’s or any family member’s device. In case it doesn’t recognize the devices there will be backup methods like biometric security and pass code. There will be motion detectors at the entry points in the compound and all possible entry points in the house i.e. Doors, Windows and vents. There will be cameras covering the main gates, back gates and all the possible entry points in the house.

There are at least two small bots, one in the outer compound and other inside the house. These bots are equipped with cameras, microphones and a stun gun. The bots has the ability to follow the intruders on their own or can be controlled remotely by the user. The police department will be informed about this project, so in case someone breaks in the house then the system will inform the nearest police station about the same.
4.3 Working

When someone enters the main compound then the motion detectors at the main door will activate the cameras, in case the person does not use the main gate instead sneaks in over the boundary then for such case there are motion detectors at every possible entry point in the house, which will activate the cameras if it detects any motion. Now the facial [11] and voice [12] recognition system will try to identify the person, if it finds a match in its database then the system will only inform the owner about the event. If the system does not find a match but the person unlocks the gate normally, i.e. by using the pass code or any biometric security [13] method then it informs the owner and activates the bot inside the house, which will capture the activities of the unidentified persons. But, if the unidentified person tries to break in then the system informs the user, nearest police station, and will activate the bots [14]. There are two bots one in the outer compound and other in the house, the bot in the house will start to follow the person, discretely recording and uploading the audio visual feed to the server and the owner in real time [15][16]. If the owner notices this notification then he/she can take control of the bot and the security systems of the house remotely. The stun gun of the bot can be only activated remotely [17], it can’t be activated by the system. Meanwhile the bot in the outer compound will patrol the compound to check if there are any more intruders. Now, as the intruder exits the house the bot in the outer compound will start to follow the person even if he/she leaves the property, and will continue to follow till its batteries allow, and then will return back to the property.

Fig. 2 DFD of the smart house security system

5. Problems

The most dangerous problem is the threat from hackers. People with some knowledge and skill can break through the entire security system and render all this security measures useless.

A problem that arises with having different IOT [18] products is that each product has its individual cloud network which consist of individual database in which the data gets stored and retrieved when required. Also for transmission of data from the agent to the user device (say computer or smart phone) there exist a server (physically located somewhere) for every individual product [19]. This increases the cost of buying cloud space and setting up servers for each and every product. Also there is a huge consumption of resources and energy which would not be considered efficient. Another drawback of having multiple servers and cloud space is that it needs multiple software’s and applications to send and retrieve data. Henceforth it increases the overall complexity and cost of setting up a smart environment.

These are some problems with implementing Internet Of Things Technology.

6. Solutions

The solution to the first problem can be using high level encryption [20] in data transfer, or another solution can be rebooting the system which may raise some other problems.
The solution for the second problem i.e. having multiple IOT products which uses different cloud and apps is that to use a centralised cloud system [21] having multiple database that can manage data for different IOT devices, syncing all the devices to the same cloud. The idea is to have a single app for all the IOT devices and the smart house.

These can be some possible solutions but more research is definitely needed in these growing fields.

7. Conclusion
The core motive of this paper is to provide an idea about Internet of Things and related devices. Also, this paper provides a brief idea about the possibilities and capabilities for improving the important aspect of our daily life in the near future.

In this paper, the issues of home security have been raised and a futuristic idea and set of solutions has been proposed. The possibilities are endless and with the help of advancements in software technology and new upcoming engineering modules, the Internet of Things can be a boon and a revolutionary technology that can shape this world in a manner that is beyond imagination and wasn’t recently possible.

References
[1] N. Kumar, A. Agrawal, R. A. Khan, “METHWORK: An Approach for Ranking in Research Trends with a Case Study for IoET, Recent advances in Computer Science and Communication (formerly Recent Patents on Computer Science), 2019.
[2] N. Kumar, A. Agrawal, R. A. Khan, “IoT based Alert Network for Flood Genera Emergencies”, in 3rd IEEE conference on Research in Intelligent and Computing in Engineering (RICE-2018), at University Don Bosko, El Salvador, Central America, Online in Nov. 2018.
[3] Automatic Door Locking System, Neelam Majgaonkar, Ruhina Hodekar, Priyanka Bandagale, 2016 IJEDR | Volume 4, Issue 1 | ISSN: 2321-9939
[4] The Digital Locking and Unlocking System, Prof. Pratima Patel, Prof. Samir Ajani, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 2, February 2016 ISSN: 2277 128X
[5] Security in the Internet of Things: A Review, Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, 2012 International Conference on Computer Science and Electronics Engineering
[6] Automated Facial Expression Recognition System, Andrew Ryan, Jeffery F. Cohn, Simon Lucey, Jason Saragih, Patrick Lucey, & Fernando De la Torre, Adam Rossi
[7] Automatic Speech Recognition, Preeti Saini, Parneet Kaur, International Journal of Engineering Trends and Technology- Volume4Issue2- 2013
[8] Development of Microcontroller-Based Biometric Locker System, Crystalynne D. Cortez, Jaswinder S. Budwal, Jocelyn R. Hipolito, Ditche Jane C. Astillero, Melvie S. Dela Cruz, and Jaira C. Inalao
[9] Wireless Controlled Surveillance Robot, Kunal Borker, Ajaysingh Rajput, International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 2, February 2014, ISSN: 2321-7782
[10] Real Time Video Monitoring System Using Raspberry Pi, Sunidhi Kanzariya, Prof. Vishal Vora, National Conference on Emerging Trends in Computer, Electrical & Electronics (ETCEE-2015) International Journal of Advance Engineering and Research Development (IAERD) e-ISSN: 2348 - 4470 .print-ISSN:2348-6406.Impact Factor:3.134
[11] Real Time Remote Video Monitoring System Based on Embedded Web Technology, Aparna Thomas, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 4, Issue 3, March 2015
[12] Remote Control Behavior of Bots, Elizabeth Stinson and John C. Mitchell
[13] A Review on Internet of Things (IoT), M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Anjum Khairi
[14] Changes and Opportunities of Internet of Things, Yen-Kuang Chen, semanticscholar.org
[15] Cryptography Secure Against Related-Key Attacks and Tampering, Mihir Bellare and David Cash and Rachel Miller
[16] Centralized Database Security in Cloud, Leena, Miss A.Kakoli Rao, International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 8, October 2012
[17] Galil, M., Timan, T., & Koops, B. J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. Philos & Technology, 30(1), 9-37.
[18] Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), 164.
[19] Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014, November). IoT security: ongoing challenges and research opportunities. In 2014 IEEE 7th international conference on service-oriented computing and applications (pp. 230-234). IEEE.
[20] Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. International Journal of Communication Systems, 25(9), 1101.
[21] Gubbi, J., Buyya, R., Manusie, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.
[22] Neeraj Kumar, Paresh Goyal; Gayatri Kapil; Alka Agrawal; Raees A Khan, “Flood Risk Finder for IoT based Mechanism using Fuzzy Logic”, Materials Today: Proceedings, Elsevier, 2020.
[23] Kumar, Neeraj, Alka Agrawal, and R. A. Khan. "Cost estimation of cellularly deployed IoT-enabled network for flood detection." Iran Journal of Computer Science, issue 2, no. 1 (2019), Springer Nature: 53-64.
[24] G. Arora, A. K. Maurya, N. Kumar, A. K. Mishra, “Application of big data generated by IoT environment for HealthCare using Voice Recognition”, International journal of research in engineering, IT and Social Sciences, vol.-08, issue-11, November 2018, page. 132-136.
[25] Singh, Prabhuneek, and Raj Shro. "A New Computationally Improved Homomorphic Despeckling Technique of SAR Images." International Journal of Advanced Research in Computer Science 8.3 (2017).
[26] Kidwai, Abdullah, et al. “A comparative study on shells in Linux: A review.” Materials Today: Proceedings (2020).
[27] Singh, Mehal, Prabhuneek Singh, and Pramod Kumar. “An Analytical Study on Cross-Site Scripting.” 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA). IEEE, 2020.