ISSN:0975-9646

Challenges of Internet of Things; the Invention and Implementation of a Theoretical Context

Z. H Abdullahi[1], Shailendra Kumar Singh [2], Nuhu Alhaji Muhammad[3] Muhammad lawan[4]

[1]Research Scholar, Department of Computer Science and Engineering, Lovely Professional University, Punjab, India
[2]Assoiate. Professor, Department of Computer Science and Engineering, Lovely Professional University, Punjab, India
[3] Department of Electrical Engineering, Kano State Polytechnic, Kano Nigeria
[4]Computer Science Deparment, Hussaini Adamu Federal Polytechnic Kazaure, Nigeria

hassanzakariyya78@gmail.com

Abstract— The purpose of this paper is to discuss the potential of the internet of things and the primary challenges it faces, like threats to personal information, government surveillance, and cybercrime. This is a theoretical paper that advances testable hypotheses based on a technological overview and an examination of existing literature. This paper concludes the challenges of the internet of things that can be overcome by adhering to the conceptual framework discussed in this paper. This framework recommends that users read privacy policies, create strong passwords, collaborate with manufacturers to ensure proper security, and collaborate with the government to enact strict laws against it. This paper has conceptualised the challenges of the internet of things and the steps that can be established to resolve the issues. If users, manufacturers, and the government follow these steps, then the challenges faced by the internet of things can be solved to some extent.

Keywords— Internet of things (IoT), Personal Privacy, Government surveillance, Cyber crimes

I. INTRODUCTION

In today's modern era the advancement of technology has made our lives easier, convenient and comfortable, Internet of things is one of the important part of that advancement [1]. Internet of thing is a computing concept that describes the idea of everyday physical object being connected to the internet and being able to identify themselves to other devices [2]. Device like watches, TV, Fridge, car etc. all are connected to internet, and this is internet of thing. For example, a watch, traditional watches were used only to see time but since internet of thing concept came in the market, people have started using smart watches. These smart watches are connected with internet and smartphones. Smart watches track heart rate, sleep activity and overall fitness level. But IoT is a diverse and complex network, any failure or bugs in the software or hardware will have serious consequences [3]. Internet of thing is making our life comfortable but there are many challenges that we need to resolve and for developing trust in mind of users, government need to make strict rules and regulations [4]. With the emergence of internet of things, new regulatory approaches are required to ensure the privacy and security of users [5]. Some of the main issues are how to make computer system or software to exchange information safely and make use of information with interconnected. Devices which is called full interoperability. Furthermore, how to make them smart enough so that they can guarantee trust, security and privacy of the users and other data [6]. The IoT framework is likely to be influenced by attacks at each layer hence there are many issues and requirements needed to be addressed. And with the rapid advancement of technology, it is essential to incorporate new network protocol like IPv6 and 5g to achieve the dynamic mashup of the topology [7]. Internet is the foundation of IoT, IOT devices work through internet. Hence all the security threat that lie within internet propagate to IOT as well. Furthermore, with fast development and increasing use of IOT devices in our daily lives indicates the importance to think and begin to deal with these security threat before deployment [8]. Reason for the increased security risk in IoT is that connection among devices are usually carried out using open wireless links which offer limited privacy in communication. And it is also considerable that network devices have limited processing and storage capacity and do not run powerful operation system, thus complicated intrusion detection schemes, virus scanners and other traditional security defense mechanisms cannot be supported [9]. Beyond other challenges, the important question is at which level to base the security in the IoT. The link layer, the network layer as well as the application layer. In all these layers the security requirements and communication patterns are different and in small devices resources are limited that makes challenging to secure all layers individually [10]. All these papers have discussed various challenges of IoT and have also given some suggestions to solve these problems. But none of these papers have specifically discussed about personal privacy issues, Government surveillance and cyber-crimes threats. And presently these three problems are the main problems we are facing due to IoT. So, in this paper these problems have discussed in detail and have also given some suggestions to solve these problems.

II. ISSUES FACED BY INTERNET OF THINGS

A. Personal privacy is at risk:

Personal privacy is a crucial aspect of our lives and a basic human right [11]. When we are happy, we like to share what we have with our family, relatives, and friends. And when we have problems in our lives, we talk about them with our loved ones. We enjoy sharing personal information with folks we care about and are familiar with. We also have some personal information we don't

wish to share with anyone. Privacy isn't about keeping things private or keeping secrets hidden; it's about having a say in what we tell other people. And the internet of things infringes on our privacy because these devices allow anyone to learn about someone's personal life. Everything linked to your personal life, such as what we do, where we go, who we talk to, e-mail texts, the type of material we search on the internet, and our credit card number, is easily accessible [12]. We are all connected to a variety of internet of things devices in today's world. These devices have made our lives easier while also causing some big issues [13]. Roomba is a robot vacuum cleaner. I Robot sells a series of self-contained vacuum cleaners. It also has the capacity to create a map of your home and locate anything within it. After some time, the company stated that these maps would be shared with commercial partners [14]. Many tech corporations, such as Google, Amazon, Apple, and Facebook, can utilize this information to find out what is going on inside your home and easily intrude in your personal life. And if hackers gain access to these companies' computer systems, your personal information could fall into the wrong hands. Thieves can steal items from your home using this information, putting your family's safety in jeopardy. The hacker can then listen in on your phone conversations, read your emails, and obtain bank information such as credit and debit card numbers. He has access to all of your IoT gadgets, including your phone, laptop, automobile, Wi-Fi kettle, smart locks, and so on. As a result, this is how IoT devices infringe on our privacy.

B. Surveillance by the government:

The government asserts that monitoring is used for the welfare of society. However, the government does not always employ it for the benefit of society [16]. Surveillance is sometimes used by the government for its own profit. During election season, the government may use it to track voting trends and learn more about what people believe about government, such as how many people support or oppose it. The most serious downside of monitoring is that we may lose our privacy as a result of government control [17]. Because the government has complete control over all messages, privacy, and personal information. In addition, Internet of Things devices will expand government surveillance. Even the tiniest gadgets, such as smart watches, are connected to the internet in today's modern world. Smart watches appear to be highly popular these days. Heart rate, sleep activity, and overall fitness are all monitored by smart watches. It can play music and perform other tasks without the use of a phone. Imagine you're sitting in your living room watching TV when the cops arrive at your door and inform you that you've been fined for driving while inebriated. According to a study done by Bangor University, Smart watches appear to be highly popular these days. Heart rate, sleep activity, and overall fitness are all monitored by smart watches. It can play music and perform other tasks without the use of a phone. Imagine you're sitting in your living room watching TV when the cops arrive at your door and inform you that you've been fined for driving while inebriated. According to a study done by Bangor University,

C **Cybercrimes:**

The 2016 Dyn hack is an example of how internet of things devices are increasing the danger of criminality. The 2016 Dyn hack was a series of distributed denial of service (DDoS) assaults that began on October 21, 2016, and targeted Dyn's DNS services. Large swaths of users in Europe and North America were unable to access key Internet platforms and services as a result of the assault. The hacker collectives Anonymous and New World Hackers claimed responsibility for the attack, however there was little evidence to back up their claims. Dyn, as a DNS provider, offers end-users with the service of translating an Internet domain name to its matching IP address when typed into a web browser, for example.

A massive number of DNS lookup requests from tens of millions of IP addresses were used to carry out the distributed denial-of-service (DDoS) assault. The attacks are thought to have been carried out by a botnet made up of a huge number of Internet of Things devices infected with the Mirai malware [19], such as printers, cameras, home gateways, and baby monitors. Other examples include the WannaCry ransomware assault and the theft of a Bangladesh bank; in all of these cybercrimes, internet of things devices was used. And unless preventative measures are done, this will continue in the future.

III A THEORETICAL ARCHITECTURE

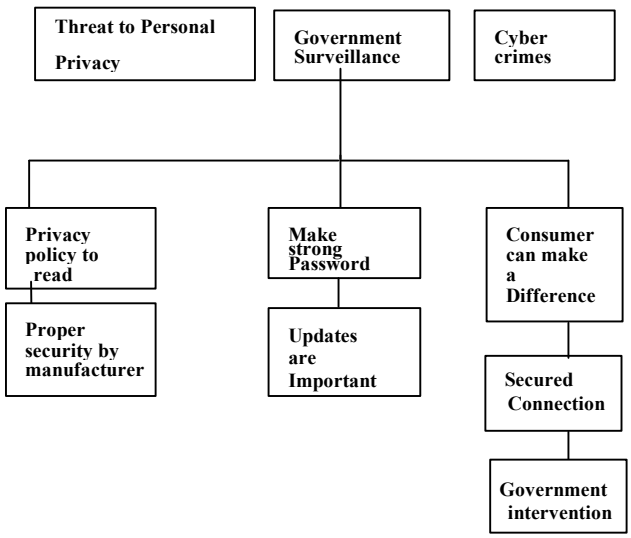

Fig 1 Theoretical Architecture

To explore the problems with the Internet of Things and recommend relevant solutions, a theoretical model has been established in Figure 1.

A **Privacy policy to read:**

Most people don't read privacy policies, which are crucial for protecting individual privacy. Perhaps there won't ever be a breach of privacy if consumers take it seriously. But both parties are making a mistake. Users ignore the privacy statement because they are too lazy to read it. The lengthy and pointless service terms of service providers are the real culprit for people not reading privacy policies, though. The privacy statement contains some irrelevant information, such as the conditions for signing up for the

website's email newsletter or the way the website manages the personal or financial data of users who make donations or sales there. Users merely want to know what kinds of files and information service providers need to access in order to perform their functions, as well as where and with whom they will share it. Users will read the policy and be aware of where their information is being shared if service providers make their privacy policies accessible and succinct by utilizing straightforward language. The General Data Protection Regulation in Europe states that a privacy notice must be "clear and straightforward English," "concise, visible, indelible, and easily accessible," but the majority of privacy notices do not adhere to these specifications

B, Proper security by Manufacturers

If manufacturers produce high-quality products with no security issues, among other things, users won't ever experience a privacy infringement problem. An example of this is Kayla, an interactive children's doll. She is able to hear what children are saying and answer their inquiries. If it is hacked, a person could spy on children or communicate with them. It had subpar security features and was later outlawed in many nations. Therefore, it is the manufacturer's responsibility to provide secure features that end users can then utilize

C, **Make strong Password:**

A secure password and user name must be created when using an app or signing up for a website. To put it simply, we must create an account before using their services. The service providers ask for access to your personal information, documents, and data when we create an account on a website or an app. Then they save in their system all the data related to that account. Someone can access your personal information if he discovers your password. The same condition is with IoT devices, when we use IoT devices, we need to secure our device with a strong password. And if the password is not strong enough then hackers can easily hack the device and can get access to our personal information. So, it is important to set some password that so strong and not easy to guess. The best password is the one that contains uppercase letter, lower case letter, number and special characters. The longer it is the better

D Updates Are Important:

The security of gadgets connected to the internet is constantly being breached by hackers. However, if devices keep upgrading after a set amount of time, it becomes more challenging for hackers to compromise the device's security. Over time, updates give devices new capabilities in addition to patching security problems. To protect the security of gadgets, manufacturers should release updates at regular intervals**.**

E Consumers Can Make Difference:

Customers who purchase IOT devices will need to be cautious. They must determine whether the machinery is of high calibre, whether it offers robust security, and whether the producer offers the capability of updating it. These questions must be answered for consumers. Customers should submit their experiences on the company's website if they discover after purchasing the item that it is of poor quality and is not secure so that the manufacturer may make the necessary corrections. Manufacturers will be encouraged to produce high-quality and secure devices if consumers become aware of them and cease purchasing devices with inferior functionality and security.

F. Secured connection:

On the market, there are some operating systems that guard IOT devices from security lapses. One of them is the free RTOS (real-time operating system) from Amazon, which makes small, cutting-edge devices simple to manage, deploy, connect, and secure. It includes libraries for data encryption as well as others to assist safeguard device data and communications. It facilitates the safe connection of devices to the cloud [20]. data and transmits it to the relevant internet resource, like your company's intranet, a web server, or an email server. The data is then sent from the internet resource back to a location within your VPN network, where it is encrypted. A different location in your VPN network receives the encrypted data and decrypts it before sending it back to your client machine via the internet. [22] One such operating system is the free open-source embedded MBED OS, which was created exclusively for Internet of Things (IoT) devices [21]. It offers multiple layers of protection to guarantee that personal data is not compromised. Using a VPN is another way to serve the internet safely (virtual private network). A virtual private network (VPN) is a set of virtual connections that are routed over the internet and encrypt data while it is transferred back and forth between your client computer and the internet services you are utilising, including web servers. Such internet protocols as HTTPS, SSH, NNTPS, and LDAPS all provide built-in encryption.

G Government Intervention:

To guarantee the defence of IOT devices from hacking, the government must create new regulations. Manufacturers must be required by law to disclose to customers how secure their products are, and they should only be permitted to sell goods that meet a predetermined standard for security. New legislation and regulations for internet of things devices are being developed by organizations like the European Consumer Organization and the Norwegian Consumer Council. The UK government recently unveiled new regulations to safeguard IOT devices. Government oversight of internet of things device security will increase pressure on manufacturers to release products with high levels of security.

IV. Digital Forensics Investigation

Digital forensics is the act of gathering, evaluating, analyzing, and presenting the evidence to a court. While IoT forensics uses a variety of smart devices, most often smartphones and other connected devices, traditional forensics relies on PCs. More research is required to create frameworks and guidelines for practitioners in such a volatile environment.[27]

V. Traditional Forensics Investigation

Data is obtained in traditional forensics from sources such as hard drives, RAM, system logs, or any peripheral

storage. For deeper investigation, the examiner can use techniques such as file carving in unallocated space. After the data acquisition, the collected artefacts are analysed from a technical and legal perspective.[28]

VI. CONCLUSION

We are surrounded by Internet of Things (IoT) gadgets in the current era, and as technology advances, so will their use. It is currently only used in a few industrialized nations, but in the future, poorer nations will also use it more frequently. However, wherever it is used, individuals must deal with connected issues. An illustration of it is the 2016 Dyn attack, which utilized IoT devices to carry out the attack. Many internet services were temporarily shut down as a result of it, and social media sites like Twitter suffered significantly. Threats from cybercrime, invasions of personal privacy, and government spying are the primary issues that have gotten worse with its use. Therefore, all of these issues have been thoroughly discussed in this research along with recommendations for how to make them less severe. private matters, which entails We all have private knowledge that we either don't want to share with anyone or that we like sharing with our loved ones. IoT gadget use, however, undermines our right to privacy. If we carefully read the service policies before utilizing any services, we can prevent it from happening. also by checking the number and caliber of security features the service provider offers. The prevention of cybercrimes is the second major issue, and here the manufacturer may make a significant contribution. Hackers cannot access equipment if the maker supplies them with plenty of security features. The IoT also presents us with the dilemma of growing government surveillance. Government monitoring entails that the government is watching us. It now has certain benefits, such as making it simple for the government to track down and manage criminals. However, it also has certain drawbacks because it keeps us constantly under government surveillance. which is a privacy violation. Additionally, the government can use it for its own gain, such as during elections to determine how the population feels about the incumbent government. and get others to consider the opposing viewpoint. The biggest illustration of this is the 2016 US presidential election. Some candidates in this election used social media to keep an eye on voters. Now, the government is the only one with power over it. To ensure that surveillance is exclusively carried out for the benefit of society, the government should enact stringent regulations.

REFERENCES

1. A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno, “A decentralized approach for security and privacy challenges in the Internet of Things,” in 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea (South), 2014, pp. 67–72.
2. “What is the Internet of Things (IoT)? - Definition from Techopedia.” [Online]. Available:https:// www.techopedia.com/definition/ 28247/int ernet-of-things-iot. [Accessed : 14-Aug2019].
3. T. J. Gerpott and S. May, “Integration of Internet of Things components into a firm’s offering portfolio – a business development framework,” INFO, vol. 18, no. 2, pp. 53–63, Mar. 2016.
4. S. Chatterjee and A. K. Kar, “Regulation and governance of the Internet of Things in India,” Digital Policy, Regulation and Governance, vol. 20, no. 5, pp. 399–412, Aug. 2018.
5. R. H. Weber, “Internet of Things – New security and privacy challenges,” Computer Law & Security Review, vol. 26, no. 1, pp. 23–30, Jan. 2010.
6. D. Bandyopadhyay and J. Sen, “Internet of Things: Applications and Challenges in Technology and Standardization,” arXiv:1105.1693 [cs], May 2011.
7. R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, “Internet of things (IoT) security: Current status, challenges and prospective measures,” in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, United Kingdom, 2015, pp. 336–341.
8. I. Andrea, C. Chrysostomou, and G. Hadjichristofi, “Internet of Things: Security vulnerabilities and challenges,” in 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 180–187.
9. D. Chasaki and C. Mansour, “Security challenges in the internet of things,” IJSSC, vol. 5, no. 3, p. 141, 2015.
10. T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, “Security Challenges in the IP-based Internet of Things,” Wireless Pers Commun, vol. 61, no. 3, pp. 527–542, Dec. 2011.
11. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.
12. J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, “Privacy in the Internet of Things: threats and challenges,” Security Comm. Networks, vol. 7, no. 12, pp. 2728–2742, Dec. 2014.
13. S. A. Kumar, T. Vealey, and H. Srivastava, “Security in Internet of Things: Challenges, Solutions and Future Directions,” in 2016
14. 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 2016, pp. 5772–5781. A. Allan, “The coming privacy crisis on the Internet of Things | TEDxExeterSalon - YouTube.” [Online]. Available: https://www.youtube.com/watch?v=yG4JL0ZRmi4&t=15s.[Accessed : 13-Aug-2019].
15. K.Munro,“InternetofThingsSecurity | TEDxDornbirn - YouTube.” [Online]. Available: https://www.youtube.com/watch?v=pGtnC1jKpMg&t=1s. [Accessed: 13-Aug-2019].
16. Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, “A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities,” IEEE Wireless Commun., vol. 20, no. 6, pp. 91–98, Dec. 2013.
17. M. Amadeo et al., “Information-centric networking for the internet of things: challenges and opportunities,” IEEE Network, p. 9, 2016. Y.Elovici,“HowdangerousareITdevices?|TEDxBGU-YouTube.” [Online]. Available: https://www.youtube.com/watch?v=vgoX_m6Mkko&t=363s. [Accessed: 13-Aug-2019].
18. “2016 Dyn cyberattack,” Wikipedia. 10-Aug2019.
19. “Amazon FreeRTOS - IoT operating system for microcontrollers - AWS.” [Online]. Available: https://aws.amazon.com/freertos/. [Accessed: 14-Aug-2019].
20. “MbedOS|Mbed.”[Online].Available:https://www.mbed.com/en/platf orm/mbedos/. [Accessed:14-Aug-2019].
21. K. Crawley, “How Does a VPN Work? Explain VPNs to me | AT&T Cybersecurity | AT&T Cybersecurity.” [Online]. Available: https://www.alienvault.com/blogs/securityessentials/explain-how-vpn -works. [Accessed: 14-Aug-2019].
22. Alabdulsalam S, Schaefer K, Kechadi T, Le-Khac NA (2018) Internet of Things forensics:challenges and case study. https://www.researchgate.net/publication/322851720_Internet_of_ things_forensics_Challenges_and_Case_Study
23. Bakhshi T (2019) Forensic of Things: revisiting digital forensic investigations in Internet ofThings. In: 2019 4th international conference on emerging trends in engineering, sciences and technology (ICEEST), Karachi, Pakistan, pp 1–8. https://ieeexplore.ieee.org/abstract/doc ument/8981675