International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

# Challenges of Internet of Things: Development and Application of Conceptual Framework

**Harvinder Singh, Abhishek Sharma**

***Abstract*: The purpose of this paper is to discuss the potential of internet of things and primary challenges like threat to personal information, Government surveillance and cybercrime faced by internet of things. This is conceptual paper that advances testable preposition based on the the technological overview and use of existing literature review. This paper concludes the challenges of internet of things that can be resolved by following the conceptual framework discussed in this paper. This framework suggests users to read privacy policy, make strong password, and manufacturers to provide proper security and government to make strict laws against it. This paper has conceptualised the challenges of internet of things and the steps that can be established to resolve the issues. If users, manufacturers and government follow these steps then the challenges faced by internet of things can be solved with 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, 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.

Manuscript published on 30 September 2019
* Correspondence Author
**Harvinder Singh*,** Associate Professor, Mittal School of Business, Lovely professional University, Jalandhar, Punjab India, E-mail: hsingh_07@hotmail.com
**Abhishek Sharma.** Research Scholar, Mittal School of Business, Lovely Professional University, Jalandhar, Punjab IndiaE-mail: Thetycoonsharma@gmail.com



## II. ISSUES FACED BY INTERNET OF THINGS:

### A. Threat to personal privacy:

Personal privacy is an important part of our life, it is a fundamental human right [11].

We humans like to share when we feel happy, we share things with our family, relatives, and friends. And when we face difficulties in our life then we share those troubles with our loved ones. We like to share our personal information with those who are close to us and whom we know. And there is some personal information that we do not want to share with anyone.

Privacy is not about keeping things private, it is not about secrets, it is about choice, the choice what we tell other people ourselves. And internet of things violates our privacy, anyone can know about someone's personal life through these devices. All the things that our related to your personal life like what do we do, where do we go, who do we talk to, e-mail texts, kind of information we search on internet and our credit card number, everything can be easily known [12]. In today's modern age we are connected to a lot internet of things devices. These devices have made our life comfortable and have also created some major problems [13]. There is a device name Roomba, it is a series of autonomous vacuum cleaner sold by I Robot. It also has ability to make map of your home and it finds out where things are in your home. After sometime its manufacturer gave a statement that they would share these maps with their commercial partners [14]. By doing this many tech companies like Google, Amazon, Apple, Facebook, can find out what is happening inside your house and can easily interfere in your personal life. And if hackers get into these companies' computer system then your home information may be in the hands of wrong people. With the help of this information thieves can steal things from your house, and it also puts the security of your family members in danger. One more device called 'Smart Padlock', it uses finger prints to lock and unlock things. But researcher discovered that it can be locked and unlocked by other ways. Anyone who has some technical knowledge can open it easily through Bluetooth. So, it is also not secured and we cannot trust it completely. One more device called 'Wi-Fi kettle'. It boils water with the help of an app installed on smartphone and it can be operated from anywhere in the home or office. But researchers have found that it can also be easily hacked. And if someone hacks the Wi-Fi kettle then he can also find out our Wi-Fi password [15]. Then hacker can listen your mobile talk, see your mail text and find out bank details like credit and debit details. He can control all the IOT devices you are using like mobile, laptop, car, Wi-Fi kettle, smart padlock etc. So, this is how IOT devices violate our privacy.

**B. Government Surveillance:**

Government always claims that it uses surveillance for the betterment of the society. But government does not always use it for the welfare of the society [16]. Sometime government uses surveillance for its own benefit. At election time government can use it to know the voting trend and tries to know what people think about government, how many people are in favor or disfavor of government. The biggest disadvantage of surveillance is we may lose our privacy because we our under the control of government [17]. Because all the messages, privacy and personal information are controlled by the government. And the IoT devices will increase government surveillance. In today's modern era, even the smallest devices are connected to internet for example the smart watches, smart watches seem to be very common nowadays. Smart watches track heart rate, sleep activity and overall fitness level. It can play music and do phone free activity. Now imagine you are sitting in your house and watching Tv, suddenly police knock on the door and tells you that they have fined you because you drove while you were intoxicated. A research conducted by Bangor university, where researcher found that smart watches can find out whether you are intoxicated or not. Now question arises that how come police know that I was driving when I was intoxicated. As I said before, nowadays cars are also connected to internet. Cloud provider of these connected car there is knowledge when I drove. If we corelate the data from the smart watch together with the data from connected car platform you know that I drove actually when I was intoxicated [18]. This is just one example another example is, if your friend commits a crime, which you do not know about. And you talk to him, you go to his house to meet him and you invite him to your house for dinner. Everyone he knew, everyone he worked with will come under suspicion so now you will also come under suspicion. Since you are very close to him, police will ask a lot of questions from you, and you will have a lot of trouble. Now how police know about you and how close you are with your criminal friend. The answer is through internet of things devices, car on which you went to meet him, mobile on which you were talking to him all are connected to internet. And government keeps taking information from cloud service providers of these IoT devices to keep an eye on everyone. This is how IoT will increase government surveillance which harm our personal privacy.

**C. Cybercrimes:**

Internet of things devices are increasing the risk of cybercrimes, 2016 Dyn cyberattack is an example of this. The 2016 Dyn cyberattack was a series of distributed denial of service (DDoS attacks) on October 21, 2016, targeting systems operated by Domain Name System (DNS) provider Dyn. The attack caused major Internet platforms and services to be unavailable to large swathes of users in Europe and North America. The groups Anonymous and New World Hackers claimed responsibility for the attack, but scant evidence was provided. As a DNS provider, Dyn provides to end-users the service of mapping an Internet domain name when, for instance, entered into a web browser—to its corresponding IP address. The distributed denial-of-service (DDoS) attack was accomplished through a large number of DNS lookup requests from tens of millions of IP addresses. The activities are believed to have been executed through a botnet consisting of a large number of Internet of things devices—such as printers, cameras, residential gateways and baby monitors—that had been infected with the Mirai malware [19] .Other examples are WannaCry ransomware attack and Bangladesh Bank robbery attack, in all these cybercrimes internet of things devices were involved. And if protective actions are not taken, this will continue to happen in the future.

## III. A CONCEPTUAL FRAMEWORK:

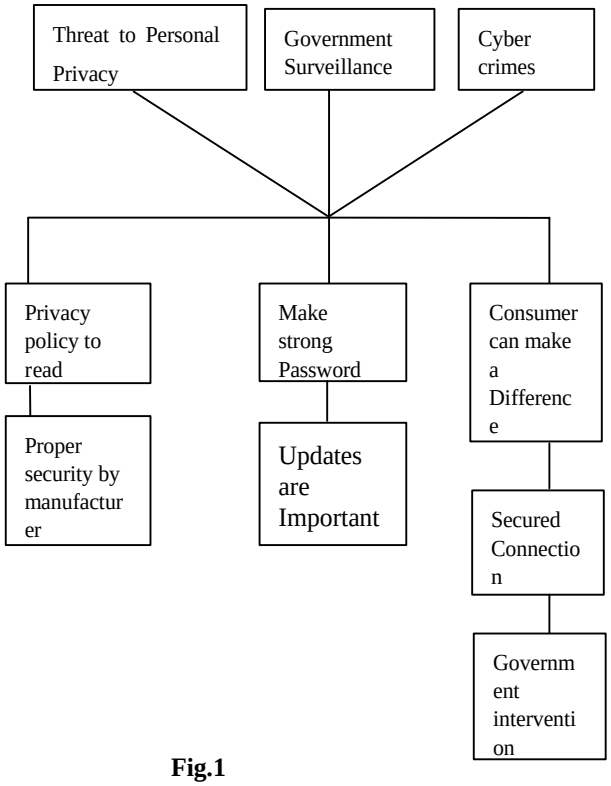


**Fig.1**

A conceptual model has been developed in figure 1, to examine the challenges of internet of things and suggesting appropriate actions to overcome these challenges.

### A. Privacy policy to read:

Most of the people do not read privacy policy which is most important for personal privacy. If users take it seriously perhaps there will never be a violation of personal privacy. But it is mistake on both sides. Users take privacy policy lightly and they feel lazy to read it. But the reason for not reading privacy policy is lengthy and irrelevant service terms of service providers. Some irrelevant things are mentioned in the privacy policy like the rule associated with subscribing to the sites email newsletter, how the sites handle personal or financial information belonging to people who make purchase or donation on the site etc. Users just want to know that what kind of documents and data, service providers need access to fulfil their functionality, and where and with whom they will share it. If service providers make their privacy policy concise and transparent by using clear and plain language then users will definitely read privacy policy and they will be aware of where it is being shared. According to Europe's general data protection regulation privacy notice must be in ''concise, transparent, indelible and easily accessible from, using clear and plain language'' but most privacy notices do not meet these requirements.

### B. Proper security by Manufacturers:

If internet of things manufacturers make good quality of devices, in which there is not possibility of security breach then user will never face privacy violation problem. An example of this Kayla, she is an interactive kids' doll. She can listen to what kids are saying and she can respond to that questions. If someone hacks it, he could spy on kids or can talk to them as well. It had poor security features and later it was banned in many countries. So, it is manufacturer responsibility to build in secure features which can then be implemented by end users.

### C. Make strong Password:

Whenever we use an app or we get registered on a website, we need to set a user name and strong password. In simple words we need to make an account then we can use their services. When we make an account on a website or an app, the service providers ask for access to your personal information, documents and data. Then they save all the information with that account in their system. An if someone figures out your password then he can get access to your personal information. 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:

Hackers always find out a new way to breach the security of internet connected devices. But if devices keep updating after a fixed interval of time then it becomes difficult for hackers to breach the security of the device. Updates add new functionality to devices over time as well as fix security flaws that need to be patched. So, manufacturer should provide updates after a fixed interval of time to ensure the security of device.

### E. consumers can make difference:

The consumers will have to be aware when they buy IOT devices. They need to see if the equipment is of good quality, does it provide strong security and does manufacture provide the facility to update it, consumers need to find the answers of these questions. And if after buying the device customers find out that the device is not of good quality and it is not secured. Then customers need to share their experiences on company's website so that manufacturer can fulfil the shortcomings. If consumers become aware and they stop buying devices with less features and security. Then this will encourage manufacturer to make good quality and secured devices.

### F. Secured connection:

There are some operating systems in the market that protect IOT devices from security breach. One of them is Amazon free RTOS (real time operating system), it is an operating system that makes small power edge devices easy to program, deploy, secure, connected and manage. It comes with libraries to help secure device data and connection, including for data encryption. It helps devices connect securely to the cloud [20].

There is another operating system that is MBED OS, it is a free open source embedded operating system designed specifically for the IOT devices [21]. It provides multilayer security which ensures no violation of personal information. There one another way to serve internet securely and that using VPN (virtual private net). A VPN is a series of virtual connections routed over the internet which encrypts your data as it travels back and forth between your client machine and the internet resources you're using, such as web servers. Many internet protocols have built-in encryption, such as HTTPS, SSH, NNTPS, and LDAPS. So, assuming that everything involved is working properly, if you use those ports over a VPN connection, your data is encrypted at least twice. A VPN connection usually works like this. Data is transmitted from your client machine to a point in your VPN network. The VPN point encrypts your data and sends it through the internet. Another point in your VPN network decrypts your data and sends it to the appropriate internet resource, such as a web server, an email server, or your company's intranet. Then the internet resource sends data back to a point in your VPN network, where it gets encrypted. That encrypted data is sent through the internet to another point in your VPN network, which decrypts the data and sends it back to your client machine [22]

**G. Government Intervention:**

Government needs to introduce new laws to ensure the protection of IOT devices from cyber-attack. Government needs to make it mandatory for manufacturers to tell consumers how secure their products are and they should only be allowed to sell product with an approved security level. There are some organisations like Norway consumer council, European consumer organisation working on introducing new laws and regulations for internet of things devices. Recently UK government has also introduced new laws for protection of IOT devices. If government intervenes time to time on internet of things device security then it will put more pressure on manufacturer to bring highly secured devices in the market.

## IV. CONCLUSION

In today's modern era we are surrounded by IoT devices and with the development of technology its use will also increase. Only a few developed countries are using it now and in the coming time, its use will also increase in developing countries. But where it is being used, people have to face problems related to it. 2016 Dyn attack is an example of it, this attack was carried out with the help of IoT devices. Due to its effect many internet services were shut down for some time and social site like twitter were badly affected by it. The main problems that have increased with its use are violation of personal privacy, government surveillance and cyber-crimes threats. So, in this paper all these problems have discussed in detail and have also given suggestions to minimize these problems. Personal privacy which means personal information that we do not want to share with anyone or we like to share with those who are close to us. But use of IoT devices are violating our personal. We can stop it from happening if we read the service policies properly before using any services. And also, by ensuring the quantity and quality of security tools the service provider is providing. The second big problem is how to prevent cybercrimes and, in this manufacturer, can play an important role. If the manufacturer provides devices that is full of security tools then hackers cannot get into these devices. And another challenge that we have to face due to IoT is increasing government surveillance. Government surveillance means government is keeping an eye on us. Now it has some advantages such as government can easily find criminals and control criminal activities. But it also has some disadvantages as it always keeps us under the watch of the government, which violates our privacy. And the government can also use it for its own benefit like government can use it to know what is the opinion of the people towards the government during election. And provoke people about the opposing side. 2016 USA president election is the biggest example of this, in this election some parties monitored the people with the help of social media. Now it can only be controlled by the government. Government Should make strict laws on this so that surveillance can be used only for the betterment of society.

## REFERENCE


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/internet-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.
6. 23–30, Jan. 2010.
7. D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization," arXiv:1105.1693 [cs], May 2011.
8. 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.
9. I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in 2015 IEEE
10. Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 180–187.
11. D. Chasaki and C. Mansour, "Security challenges in the internet of things," IJSSC, vol. 5, no. 3, p. 141, 2015.
12. 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.
13. 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.
14. 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.
15. S. A. Kumar, T. Vealey, and H. Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions," in 2016

16. 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 2016, pp. 5772–5781.
17. A. Allan, “The coming privacy crisis on the Internet of Things | TEDxExeterSalon - YouTube.” [Online]. Available:
18. https://www.youtube.com/watch?v=yG4JL0ZRmi4&t=15s.[Accessed : 13-Aug-2019].
19. K.Munro,“InternetofThingsSecurity | TEDxDornbirn - YouTube.” [Online]. Available: https://www.youtube.com/watch?v=pGtnC1jKpMg&t=1s. [Accessed: 13-Aug-2019].
20. 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.
21. M. Amadeo et al., “Information-centric networking for the internet of things: challenges and opportunities,” IEEE Network, p. 9, 2016.
22. Y.Elovici,“HowdangerousareITdevices?|TEDxBGU-YouTube.” [Online]. Available: https://www.youtube.com/watch?v=vgoX_m6Mkko&t=363s. [Accessed: 13-Aug-2019].
23. “2016 Dyn cyberattack,” Wikipedia. 10-Aug2019.
24. “Amazon FreeRTOS - IoT operating system for microcontrollers - AWS.” [Online]. Available: https://aws.amazon.com/freertos/.
25. [Accessed: 14-Aug-2019].
26. “MbedOS|Mbed.”[Online].Available:https://www.mbed.com/en/platform/mbedos/. [Accessed:14-Aug-2019].
27. 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].

## AUTHORS PROFILE

Dr. Harvinder Singh has done his Ph.D. in Marketing from Chaudhary Charan Singh University and Masters of Business administration (MBA) from University of Pune, India. He is currently associate Professor at Mittal School of Business (MHRD NIRF India Rank 52, ACBSP USA, Accredited), Lovely Professional University, Phagwara, Punjab (India). He is having 22 years of experience with blend of corporate 9 years and teaching 13 years. In academic career spanning over 13 years, He has worked as faculty at various institution in Haryana(DAV COLLEGE YAMUANAGAR, JMIT Randaur, MAIMT Jagadhari, and HEC Yamunanagar) and presently working with Lovely Professional University, Jalandhar,Punjab. He has attended 15+ relevant training and courses for continuous learning, has acted as resource person in various institutions.In corporate career of 9 years, he has worked with top blue chip companies in senior level position i.e. GOODLASS NEROLAC PAINTS LTD, JALANDHAR , STEEL TUBES OF INDIA LTD, MIMBAI, STI-SANOH INDIA LTD, INDORE, GOLDEN LAMINATES LTD, CHANDIGARH, looking after product launch, market expansion, delaer distribution channel, new product development, etc. As a researcher, he has presented several research papers in national and international conferences and seminars. He has published 10 rsearch paper in different journals like Asia Pacific Journal of Research in Business Management, Indian Journal of Marketing, Indian Journal of Public Health Research & Development, International Journal of Econmic Research, International Journal of Management, International Journals of Marketing and Technology, International Journal of Research in Commerce and Management.

Abhishek Sharma was born in Himachal Pradesh, India in 1993.He has done his Masters of Business Administration (MBA)and Masters of Commerce (M.com) from Himachal Pradesh University. He is currently a research scholar at Mittal School of Business (MHRD NIRF India Rank 52, ACBSP USA, Accredited), Lovely Professional University, Phagwara, Punjab (India). He has just started his academic career; he is doing Ph.D. in Marketing. He has one year of experience in corporate sector, he has worked as a deputy manager in ICICI BANK in Rajasthan at sumerpur district.