Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 04, April -2018

SECURITY CONSIDERATIONS FOR IoT TECHNOLOGIES

Dr.G.N.K.Suresh Babu[1] ,Dr.M.Kumarasamy[2]

[1]*Professor , Department of MCA, Acharya Institute of Technology, Bangalore-560107.*
[2] *Professor , Department of Informatics, Wollega University, Nekemte , Ethiopia.*

Abstract - *Now a days all places you can heard the word "IoT". Whether it may be in school or institutions or software organizations every one is developing programs for IoT Devices. The main purpose of this paper is how to use IoT with Secured environment. The Internet of Things can be defined as the interaction of smart objects that are connected to the Internet. In the future, IoT is going to be a part of everyone's day to day lives by extending the communication and networking capabilities of physical objects or smart devices. These devices are expected to be ubiquitous, context-aware, and deployed with some form of ambient intelligence to allow them to pool their resources and make decisions for the benefit of humanity. The terminology IoT is rapidly embracing entire societies and holds the potential to empower and advance nearly each and every individual and business. This creates tremendous opportunities for enterprises to develop new services and products that will offer increased convenience and satisfaction to their consumers. Starting from Smart Homes, Smart Health, Smart City etc., everywhere usage of IoT devices is enormous. In this paper the author deals with how we can provide more security to the IoT Devices.*

Keywords : *Sensors, Internet, Networks, Security, Attacks, Intruders*

I INTRODUCTION

Security is more important than technologies. Since more attackers or intruders attacking web sites or hacks IoT devices, the common man may not use the technology completely. Once if we are providing more security to the technologies every one can use and enjoy the benefit of technologies. Internet of Things (IoT) has attracted considerable attention during the past few years. The concept of IoT was firstly proposed by Kevin Ashton in 1999. Due to rapid advancements in mobile communication, Wireless Sensor Networks (WSN), Radio Frequency IDentification (RFID), and cloud computing, communications among IoT devices has become more convenient than it was before. IoT devices are capable of co-operating with one another. The World of IoT includes a huge variety of devices that include smart phones, personal computers, PDAs, laptops, tablets, and other hand-held embedded devices. The IoT devices are based on cost-effective sensors and wireless communication systems to communicate with each other and transfer meaningful information to the centralized system. The information from IoT devices is further processed in the centralized system and delivered to the intended destinations. The major targets of IoT are the configuration of a smart environment and self-conscious independent devices such as smart living, smart items, smart health, and smart cities among others. Nowadays the adoption rate of the IoT devices is very high, more and more devices are connected via the internet. The main goal of IoT is to create Superior world for human beings in future. Internet of Things (IoT) extends the Internet to our everyday objects, which enables new kind of applications and services. These IoT applications face demanding technical challenges: the number of 'things' or objects can be very large, they can be very constrained devices, and may need to operate on challenging and dynamic environments. However, the architecture of today's Internet is based on many legacy protocols and technology that were not originally designed to support features like mobility or the huge and growing number of objects the Internet consists of today. Similarly, many security features of today's Internet are additional layers built to fill up flaws in the underlying design. Fulfilling new technical requirements set by IoT applications requires efficient solutions designed for the IoT use from the ground up. Moreover, the implementation of this new IoT technology requires interoperability and integration with traditional Internet. Due to considerable technical challenges, the security is an often over-looked aspect in the emerging new IoT technology. Fig.1 represents the connection between IoT and other devices.

@IJAERD-2018, All rights Reserved

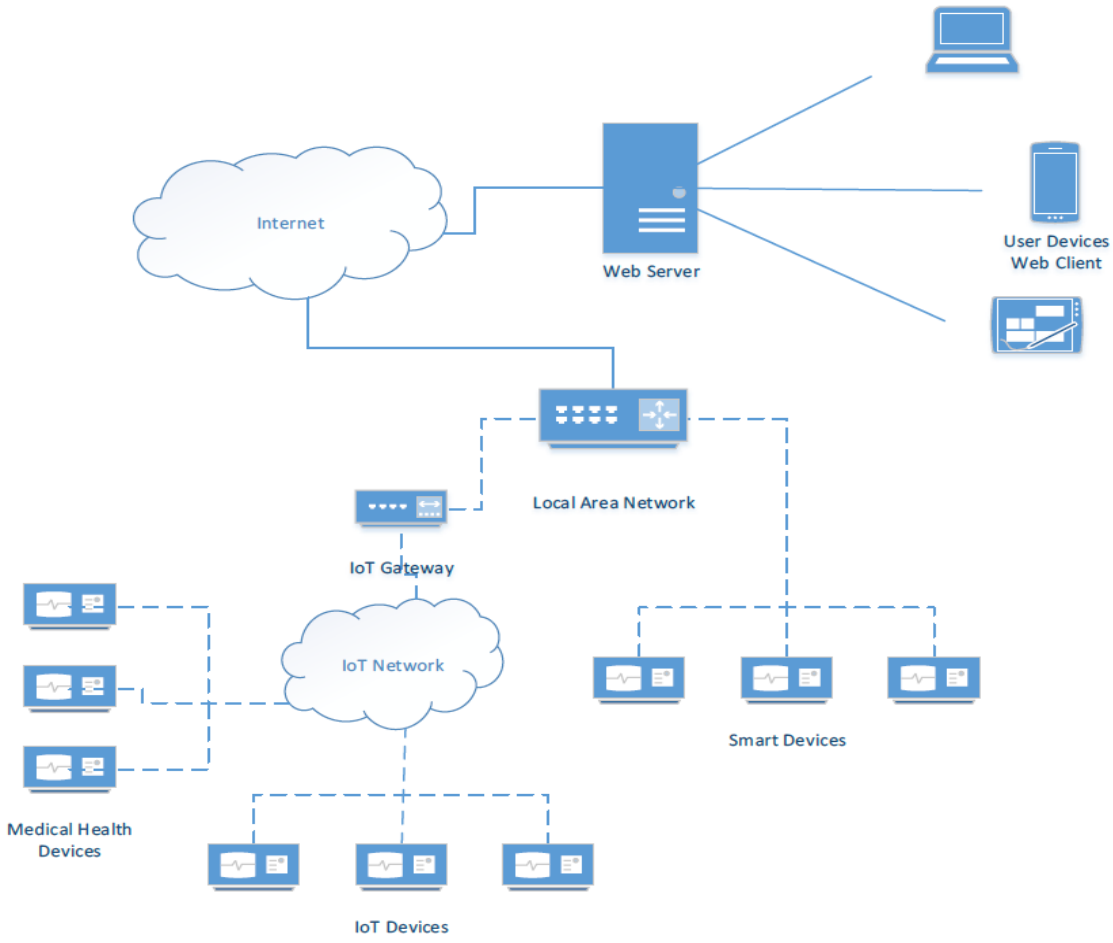

Fig. 1 IoT connect with other Devices

II CHALLENGES IN IOT SECURITY

The Internet has grown from a useful research tool for academics and industries into a fundamental utility, as important as electricity, water and gas. Wherever there is a valuable resource, there is also crime which seeks to gain value from the illicit use of that technology, or to deny the use of that resource to others. The interconnected nature of the Internet means that Internet resources can be attacked from any location in the world, and this makes cyber security a key issue. Cyber security revolves around three main themes. Confidentiality is about keeping data private, so that only authorized users can access that data. Cryptography is a key technology for achieving confidentiality. Authentication is about verifying that data has not been tampered with, and that the data can be verified to have been sent by the claimed author. Non-repudiation (i.e., avoiding denial by a sender that they actually sent a message) is sometimes considered separately, but we include it here as a subset of authentication. Access refers to only allowing suitably authorized users to access data, communications infrastructure and computing resources, and ensuring that those authorized users are not prevented from such access. Now that the Internet has become a mission-critical component of modern business, cyber security has become an indispensable component of information systems. However, as cyber security is enhanced, cybercrime is evolving to be more extensive, more destructive and more sophisticated. In Smart Homes, the ability of householders to manage their systems securely requires trusted and intuitive automated systems to assist in network management. Without such systems, the security and privacy threats of the Smart Home are likely to outweigh the advantages. Devices that previously had no communication functions are being connected to a network by IoT systems. These systems enable the discovery of phenomena that were previously unseen, providing new insights. When data gathered from connected devices is analyzed, new knowledge can be acquired. These features make the IoT a promising tool for increasing efficiency by reducing costs or increasing sales. However, in its discussion of security threats in the IoT era, the IoT Acceleration Consortium (a collaborative program with members from industry, academia, and the government) has underscored the need for measures to handle the following three issues: (1) the increasing number of network-connected IoT devices, (2) long life cycles, and (3) the difficulty of perfect manual

surveillance. In the discussion of the first issue, the increasing number of potential targets for attacks due to the increase in number of IoT devices, as well as the growing scope of influence of attacks have been pointed out. In the discussion of the second and third issues, it has been pointed out that IoT systems require little human involvement, so they can easily lapse into a situation where there is a shortage of administrators that makes attack detection difficult, and that long life cycles, over 10 years long, result in attacks that continue for long periods of time.

III NEED FOR SECURITY

IoT will impact so many different sectors and have a role in controlling physical infrastructure and services, these risks are amplified. A successful attack on an IoT device or system can have significant impact on users, device manufacturers and service providers by affecting the physical as well as the cyber world. It may expose confidential information such as private user data as well as know-how, intellectual property and process intelligence. In addition, it can lead to interruption of operations, compromise of business continuity and even danger to a company's brand image, success and very existence. For policy makers, the principal concerns related to IoT risk mitigation are the protection of public safety and privacy. It is critical that networked systems controlling industrial and public infrastructure are protected from both accidental and malicious attacks. Personal information about individuals that are monitored by IoT devices while going about their daily lives or using such devices to monitor their own property also must be protected both from accidental exposure or deliberate theft with intent to misuse. With its potential to improve traffic flow and thus both manage emissions and save fuel costs, automation of traffic management systems is a common initial project for IoT deployment in municipalities. Early implementations, however, have failed to exercise basic principles of system security and have been shown to be open to attack. While many details of this successful attack are unknown, it is likely that companies with similar automation systems are now closely examining security guidance and actual practice. A first of its kind attack that caused a loss of electrical power to customers was reported by utility companies in the Ukraine at the end of December 2015. More than 80,000 customers of at least one Ukrainian power distribution company lost service for several hours. While the cause of the outages is still being investigated, it appears that three different strategies were used to gain control of internal systems at the utility, indicating a high degree of planning involved in the attack. The rush to the IoT for home monitoring and security also appears to have outpaced principles of design for security. A vulnerability study conducted by security researchers in the summer of 2015 found serious security flaws in every one of nine Internet-connected baby monitors it tested. The researchers noted that every camera had a backdoor that would allow intruder access. Additional security flaws included the use of default passwords, easily accessed Internet portals and lack of encryption. Hackers have created web sites featuring thousands of discovered insecure webcams for curious peepers. Consumers cannot, and should not, be expected to know about and maintain the security status of net-connected home appliances. Appliances, and other devices on the IoT, must be designed with provisions for security that lasts for the lifetime of the product.

IV SECURITY ISSUES OF IOT

The key security issues in IoT is identified as follows:

- Authentication
- Authorization
- Confidentiality
- Integrity
- Privacy

Authentication

Authentication is the process of determining whether someone or something is actually who they claim to be; and not a malicious user pretending to be someone they are not. In the real world, humans do this all the time when we talk with one another; since we are able to recognize each other through various factors like facial features, hair color, voice, and so on. This identification process is not limited to humans and electronic devices also need to be aware of whom they are communicating with. For IoT, authentication is important since the majority of communications will occur without user interaction. Additionally, the ability to ensure that correct devices, sensors, and users have the right to access the network for resources and information is an important security concern. It is also crucial to ensure that information, commands, and requests are received from the correct devices.

Authorization

Authorization and access control mechanisms are used to limit the privileges that a device has and determines what actions a device is able to perform. This privilege may be in relation to, but not limited to, the access of resources and data. As a result, authorization mechanisms determine the operations each device is capable of performing and the information it has access to.

Additionally, due to the ubiquitous nature and large scale of IoT environments, it is not difficult to imagine some devices being compromised. As such, authorization mechanisms ensure a restriction on the operations an attacker is able to perform, in the event that the system is compromised. A simple example of an access control mechanism is the user accounts which individuals log into their computers under. After the initial login, which is authentication, the actions that a user can perform would be defined by the authorization controls. For instance, some users would have administrative privileges that allow them to do everything while other users are limited or restricted.

Confidentiality

Confidentiality is the means of ensuring that only the people or devices that should have access to the information, have access to that information. Ensuring the confidentiality of information is very important for IoT devices because they unobtrusively and ubiquitously collect information, which may be very sensitive in nature. As such, this is a concern because most people do not want their sensitive personal information made available for the world to see. For example: if an IoT device simply transmits all the information that it collects about your daily schedule in clear text over the Internet. Then an intruder can easily determine when would be the best time to rob your house. Confidentiality is usually achieved through the use of encryption and cryptographic mechanisms and is particularly important when IoT nodes transmit information to each other. The enforcement of confidentiality also prevents eavesdropping through cryptographic mechanisms. Fig. 2 represents the security issues of IoT.

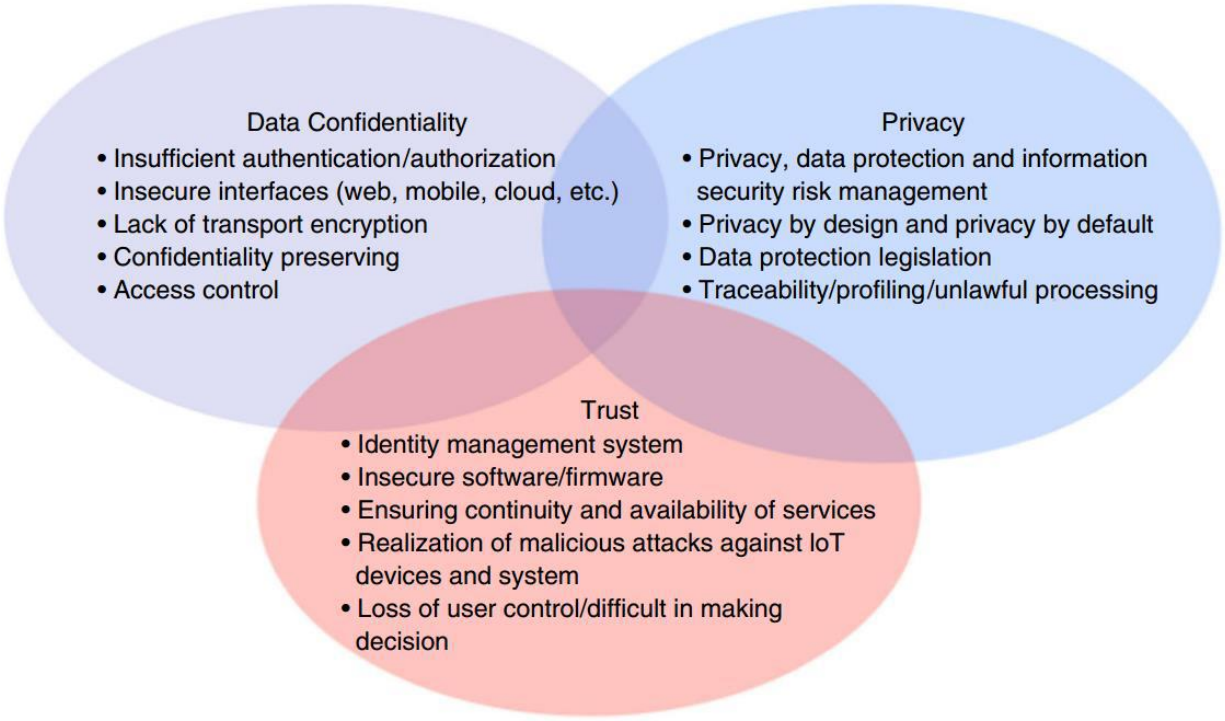

Fig. 2 Security Issues of IoT

Integrity

Integrity is the means of ensuring that the information/data is correct and has not be corrupted or modified in any way by unauthorized entities. This is usually of key importance during the transmission of information from one device to another since this is where attacks commonly occur. Data integrity is very important for IoT systems as the accurate collection of information by sensors is required for the IoT system to function correctly. As such, systems should ensure that malicious modification of data is not possible but if they occurred, the system should be able to detect it. An example where a grievous situation may arise when data is modified is in the health-care sector. Imagine if a patient is experiencing a heart-attack and a malicious individual modifies the messages sent by the sensors to say that the patient is in perfect health. Obviously this is a grave situation where the integrity of information received is of critical importance.

@IJAERD-2018, All rights Reserved

Privacy

Given the vast amount of information that IoT devices will collect about individuals, it is no wonder that privacy is of concern for the Internet of Things. This is because of the numerous privacy enforcement mechanisms developed and researched; so much so that it can be a survey on its own. Therefore we have decided to focus on the other key security concerns. Privacy can be described as "the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others". Privacy by design is one possible means of ensuring this and it is the concept whereby users use tools to manage the data that IoT devices collect about them. It is also related to the concept of ensuring that access to information is based on the least privileges required to perform an action. For example, even if a device has full access to everything on the IoT network; when it needs to perform an action that only required one resource, then the device should be limited to only using that resource while executing the particular action.

V TYPES OF ATTACKS AND ATTACKERS

When new network architecture is designed, the ideal solution is to meet as many requirements set by the users, service providers and society, but also at same time maintain a strong network security, thus keeping attackers from fulfilling their goals. For this reason, attackers are usually defined as some outsider group when describing the net-work use scenario, even though not all the attackers are the same. Examining their motives, expertise, resources and willingness to take risks, allows us to better priorities network's security requirements. Hackers, lone criminals, malicious insiders, industrial spies, terrorists and national intelligence organizations are distinctly different attacker types. Following list of different attacker types is not comprehensive.

Hackers: Real hackers have considerable expertise, often greater than that of the system's original designers. In terms of resources, they usually have a lot of time, but few financial resources. They are motivated by curiosity and desire to understand. Their willingness to take risks depends on an individual. Some of them are risk averse and some engage illegal activities with no fear of prosecution and risk involved.

Lone criminals: Lone criminals often lack expertise and resources. They don't have money or access to the system. They are motivated by financial gain and thus target commercial systems.

Malicious insiders: Malicious insiders are dangerous attackers. They may have considerable expertise and could have even been involved in the design of the system. They also have one ultimate resource. They have insider access to the system and are considered trusted. Most standard computer security measures, like firewalls are powerless against insiders, as they can simply bypass them. Malicious insiders are particularly problematic adversaries in IoT world as they require special security measures that can be hard to implement due to system limitations. The following list is compiled from most of the commonly problematic attacks against Internet of Things technologies.

Eavesdropping attack: Attacker passively monitors the communication session between two parties using the network in an attempt to determine the contents of the messages. IoT technologies use almost exclusively wireless medium at least in some parts of the network, therefore the only precondition is that the attacker is within transmission range of the communication. Attacker may even use specialized equipment, like directional antennas to eavesdrop communication outside standard specified communication range. Eavesdropping can be passive or active. During active eavesdropping, the attacker actively injects messages into the communication channel in order to assist him or her deciphering the con-tents of the messages. Many IoT applications are solely designed to transmit monitoring data over the network. This makes eavesdropping attack particularly harmful, as performing it successfully might reveal adversary all the necessary information with no need to further attack the network operation and risk detection.

Man-in-the-middle attack: Attacker positions himself or herself in between the two communicating parties. The purpose of the attack is to make both parties of the communication to believe they are communicating with each other, when in reality, they are communicating with the attacker. Successful employment of man-in-the-middle attack allows attacker to bypass cryptographic methods protecting the message confidentiality and read the plain contents of the messages. Attacker can also modify the contents of the message, thus violating the integrity of the session.

Wormhole attack: This is a variation of man-in-the-middle attack per-formed in wireless networks. The attacker connects two remotely located compromised nodes with an external connection. The compromised node listens and tunnels packets with an external connection to the location of the other compromised node, which retransmits the messages. If per-formed successfully, the other nodes in the network will misinterpret the location of the compromised node, which results in erroneous routing decisions by network's routing protocol.

@IJAERD-2018, All rights Reserved

Sybil attack: Sybil attack is another attack type performed against wire-less networks and particularly harmful against many IoT applications. In this attack, the malicious node generates an arbitrary amount of fake identities, which it claims to be able to connect to. This attack aims to corrupt routing tables of neighbouring nodes or otherwise take advantage of network accepting multiple identities. Some IoT security solutions are based on majority voting and plausibility checks, which can effectively be manipulated by multiple malicious identities.

Denial-of-service attack: As the name suggests, a denial-of-service (DoS) attack is designed to compromise service's availability to legitimate users. This is done by flooding network nodes with extensive amount of messages. Effectiveness of different flood messages varies depending on the network design and the protocols used, but the main principle remains the same. The purpose of the flood messages is to cause targeted node to instantiate data structures out of a limited pool of resources. Once the resources are exhausted, the node is unable to serve new legitimate connections, thus denying service's availability. A TPC SYN packet flooding is a popular example of a denial of service attack on IP networks. Distributed-denial-service (DDoS) attack is a variation of denial-of-service attack. DDoS attack is performed simultaneously from multiple locations.

Denial-of-sleep: In the IoT world, a battery powered network nodes can also be attacked with a specially crafted denial-of-service attack designed to exhaust device's power supply. This attack, usually referred as denial-of-sleep attack, aims to send flood messages with certain frequency in an attempt to deny a network node entering an energy saving sleep state and eventually draining the node's battery.
Attack pattern can be learned through supervised and unsupervised learning. Pattern matching algorithm for network intrusion detection and bloom filters. Bloom filters constructed using FPGA / VLSI Chips.

VI PROPOSED METHOD USING ELLIPTIC CURVE CRYPTOGRAPHY

IoT security can be more challenging to implement because it is leveraging extremely resource constrained device. A computer running a general purpose operating system like Windows or Linux will have no problem establishing an encrypted connection with another server. But a microcontroller inside a coffeemaker doesn't have the same resources and access to the same crypto stacks, and it also might not have access to enough entropy to generate truly random numbers for cryptographic keys. These are solvable problems, but they require thoughtful implementation and expertise. Elliptic Curve Cryptography (ECC) is a cryptographic concept based on elliptic curves. By using point multiplication on points on a curve and utilizing the elliptic curve discrete logarithm problem, one can achieve the same cryptographic strength as algorithms based on the prime factorization problem, such as RSA, using shorter key lengths. Different properties such as resistance to side channel attacks will differ between the curves used. When using hardware-based ECC one is usually restricted to the National Institute of Standards and Technology (NIST)-recommended curves, which has seen some controversy in recent years. There is an ongoing debate about the ownership of and patent rights to ECC which might have slowed the adoption of ECC somewhat. While ECC has many potential use-cases, it has seen the most wide adoption within Public Key Cryptography (PKC). Cryptography allows for secure communication. Attack pattern can be learned through supervised and unsupervised learning. Pattern matching algorithm for network intrusion detection and bloom filters. Bloom filters constructed using FPGA / VLSI Chips. PKI is a definition of the infrastructure and mechanisms needed to provide secure communication on an insecure network using public key cryptography. It consists of several different parts:

– A Certificate Authority
– A Registration Authority
– Directories
– Certificate Management

The basic relationship within the PKI is as follows: A company applies for a certificate through a RA that will confirm or deny the identity of the requester. If the identity is accepted, the RA will request CA to issue a certificate to the company, and also store the certificate in a certificate directory with its public key. This certificate can in turn be used to validate the identity of the company to any connecting customers or devices using the CA. If needed, the CA can revoke or renew the certificate. Security teams should take the initiative to research security best practices to secure these emerging devices, and be prepared to update their security policies as even more interconnected devices make their way onto enterprise networks.

@IJAERD-2018, All rights Reserved

VII SUGGESTIONS FOR PREVENTING THE SYSTEM

Finally the authors suggested some approaches to prevent our systems from the attackers / intruders.

- Use strong passwords to our systems i.e., combination of capital letters, special symbols and Numerals. For Ex : Jan@2018.
- Use Firewalls and Captchas.
- Use Antivirus Software and update regularly
- Deploy an Intrusion Prevention System [IPS]. [Unified Threat Management is the 64 bit high performance IPS]
- Define security policy and create awareness among users.
- Implement Application level content filtering.
- Regularly do Port, Network and Vulnerability scanning.
- Use Snort. Snort is a robust Intrusion Detection System [IDS]
- Use Kismet. Kismet is a open source wireless tools. Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs.
- Maintain log analysis and monitor if any abnormal events happen.
- Accelerate Network Testing i.e., Penetration Testing.

VIII CONCLUSION

In future, the IoT will completely change our living styles and business models. It will permit people and devices to communicate anytime, anyplace, with any device under ideal conditions using any network and any service. Securing an IT system requires confidentiality, integrity, and authorization. Security in the current Internet of Things is not as good at it ought to be. Due to limited power, bandwidth and processing power, everything needs to get stripped down to the bare minimum, while still maintaining good security properties. To ensure that the future of IoT is secure, this thesis aims to make developers think about the limitations that exists, and provide solutions to the problems that will occur when designing a device for the Internet of Things. Securing the Internet of Things is important to consumers. Through previous research it is shown exactly how devastating not focusing on the security of IoT devices can be, with the majority of consumers (62 %) "feeling completely violated and extremely angry to the point where I would take action.". Close to half (48 %) of all consumers would hold the manufacturer responsible if a flaw was to be found in the system, showing the obvious economical risks taken by not securing a device properly. The Internet of Things is a relatively new concept in terms of optimized protocols and security, and thus there is a lot of work for the future. The most pressing issue is simplifying the use of security in IoT for developers without thorough knowledge of IT security. Designing and implementing security in protocols that is simple for developers to use is a must for the future of IoT. Speed and cryptographic strength is especially important in the Internet of Things. As devices in the Internet of Things are constrained devices, efficient implementations of cryptographic algorithms is especially important to keep the cryptographic strength at an acceptable level.

REFERENCES

[1] A. Mohan, "Cyber security for personal medical devices internet of things," in Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on. IEEE, 2014, pp. 372–374.
[2] C. Li, H. Zhang, B. Hao, and J. Li, "A survey on routing protocols for large-scale wireless sensor networks.," *Sensors (Basel, Switzerland)*, vol. 11, no. 4, pp. 3498–526, Jan. 2011.
[3] D. Kozlov, J. Veijalainen, and Y. Ali, "Security and privacy threats in IoT architectures," *Proceedings of the 7th International Conference on Body Area Networks*, pp. 256–262, 2012.
[4] Evans, D. The internet of things: How the next evolution of the internet is changing everything. 2011. Available online: http://www.cisco.com/c/dam/en_us/about/ ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
[5] E. Borgia, "The internet of things vision: Key features, applications and open issues," Computer Communications, vol. 54, pp. 1–31, 2014.
[6] "Everything We Know About Ukraine's Power Plant Hack," Wired, January 20, 2016, http://www.wired. com/2016/01/everything-we-know-about-ukraines-power-plant-hack /
[7] Gartner, "Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015." http://www.gartner.com/newsroom/id/ 3165317. [Online; accessed 06-December-2016].
[8] George, F.H. The internet of things: A reality check. IEEE Comput. Soc. **2012**, 14, 56–59.
[9] Jing, L.; Xiao, Y.; Chen, C.L.P. Authentication and Access Control in the Internet of Things. In Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012; pp. 588–592.

[10] Huang, H.; Wang, H. Studying on Internet of things based on fingerprint identification. In Proceedings of 2010 International Conference on Computer Application and System Modeling, Taiyuan, China, 22–24 October 2010; pp. 628–630.
[11] IoT Acceleration Consortium Website, "IoT Security Trends," http://www.iotac.jp/wg/security/ in Japanese.
[12] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, 2014.
[13] K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.
[14] Lee, S.; Sivalingam, K.M. An efficient One-Time Password authentication scheme using a smart card. *Int. J. Secur. Netw.* **2009**, *4*, 145–152.
[15] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.
[16] N. S. Agency, "The case for elliptic curve cryptography," 2009, accessed: 15-Feb-2014. [Online]. Available: https://www.nsa.gov/ business/programs/elliptic_curve.shtml
[17] R. H. Weber, "Internet of things: Privacy issues revisited," Computer Law & Security Review, vol. 31, no. 5, pp. 618–627, 2015.
[18] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 2266-2279, 2013.
[19] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the internet of things," Future Generation Computer Systems, 2014.
[20] Want, R., Schilit, B.N. & Jenson, S. 2015. Enabling the internet of things. *Com-puter*, *48*(1), pp.28-35.URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.698.6666& rep=rep1&type=pdf. Accessed: 22 April 2017.

@IJAERD-2018, All rights Reserved