Mélange of IoT and Ransomware

Aditya Tandon

Abstract: ***The use of IoT devices are increasing rapidly. Since it integrates lots of devices, it provides lots of benefits to the users. Large companies also have started using it for coordination between the people and machines. However, Security is a major issue faced by IoT network. Trust is something that is necessary between the devices, which means that the data is transmitted without any tests to the trusted devices. IoT devices have very less security features since upgrades and patches are virtually non-existent. This makes it vulnerable to various attacks like Ransomware. Hackers will simply be able to take control of an IoT device and demand ransom for letting it go. This may get problematic especially in household devices. It is necessary to identify a solution for this this since IoT is still in the budding stage. Hence this work will analyse various available attacks in IoT and provide solutions to combat the ransomware.***

Keywords: Internet of Things, Ransomware, Security, Network, Malware, Threats

1. Introduction

Internet of Things (IoT) is entering into a promising era, where tiny devices are getting embedded into general household and commercial devices along with other sensors for sensing the data from the environment. This can be used for taking smart decisions and thereby controlling the devices to the necessity of the user. This can be done without the intervention of the humans. The number of IoT devices is estimated to cross 225 billion within 2020 and a major share of this will be wearable devices [1]. Real world applications of IoT has been increasing and smart homes that use these devices are growing. It is also not necessary that they will be implemented in smart homes only, even ordinary homes might have some independent smart devices [2]. The devices are also implemented in smart connected cars [3, 4], smart monitoring systems [5,6], intelligent parking systems [7], and intelligent meters [8, 9].

Revised Manuscript Received on July 22, 2019.
Aditya Tandon, Department of Computer Science and Engineering, Krishna Engineering College, Ghaziabad, U.P., India.

The number of cyber-attacks in the connected world are growing at an alarming rate. The attacks are targeted towards both individuals and large companies [10], Even government agencies and armed forces are not spared which has raised concerns over the security and privacy of the general public [11]. The years 2014 and 2015 experienced an alarming rate of attacks and the number of attacks has not reduced since then. The attacks are becoming more destructive in the recent times [12, 13].

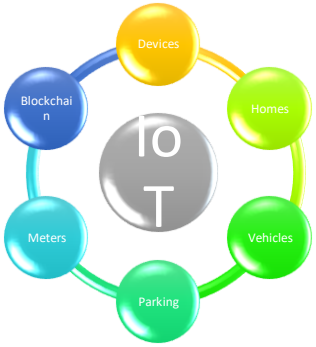

Figure 1: Applications of IoT system

Even though IoT can make the life easier for humans, there are lots of security concerns since they contain sensitive information [14]. It is estimated that around 70% of the connected devices are susceptible to cyber-attacks. Smart cars are very vulnerable to such attacks since they are a relatively new technology and contains lots of unanticipated loop holes for IoT [15]. The security market of IoT is anticipated to cross $29 billion by the year 2020 since the threats are foreseen to increase exponentially in the future. Ransomware continues to increase and it growth cannot be stopped. Hence, it has to be ensured that every device in the IoT has the ability to maintain the data confidentiality and integrity. This is necessary since ensuring this will bring better development in the IoT [16].

The conventional security measures will not be able to accommodate the IoT devices since a majority of these devices have limitations on battery and resources, therefore they need more resources for working on it [17]. The security of IoT devices have been studied in detail in different literature [18–27], however, these studies haven't discussed much in detail about ransomware which is a growing threat online.

The automated nature of most systems and low security features are major factors of success of cyber-attacks [28]. The raped entry of IoT has largely altered the features of and working of the threats [29]. When lots of these new devices are placed into force, there are lots of security risks associated which exponentially increases the threats involved [30, 31].

Retrieval Number: I33090789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3309.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

2. Challenges in IoT network

There are a lot of challenges associated with the security of the IoT platform. Making sure that the integrity of the data stays intact has become challenging since there is now lots of data and lots of devices connected together. It has to be made sure that the collected data is not compromised [32]. Eg. An attack on smart meters may report a false data and may show that the user used less power thereby creating a loss to the power company. There are lots of research to improve the attacks [33], however, they are still at an initial stage and requires more research on data integrity in IoT.

Since the IoT devices are small and lightweight, they have to compromise on other features like security and CPU power. Since the encryption techniques several watts of CPU power, it is difficult to fit the encryption techniques in the devices [34]. Therefore, lightweight security mechanisms have to be developed exclusively for these devices. Having low battery capacity is another problem since the security features increases the power consumption. The existing lightweight security techniques in [35–37] are still at its infancy and requires more research. There is also a lack of upgrades and patches to new security threats to these devices. This is due to the storage and size constraints of the IoT devices [38]. Hence, the manufacturers must look for an alternative approach to address this problem.

The manufacturers find it difficult to provide support to the devices since there are simply too much of them in distributed locations [39]. Since, there is no physical security, any attack can be made possible simply through a USB device [40]. The existing security features on the devices are primitive and with the users' intention can pose a serious threat to the entire IoT network. Providing protection physically to all the devices is very challenging.

Privacy concerns are another factor since the attacks target the private information of the individuals. Obtaining information from the devices may attract some sensitive information too which should not land in the wrong hands. In facts, the security should be built in such a way that these sensitive information must not leave the devices at all [41]. New techniques to enhance the privacy of IoT devices are discussed in [42, 43]. Another major concern is the trust, since the IoT networks are connected to other networks. Interacting with other networks with limited security features may cause problems. Hence, the existing networks must be upgraded in order to bring trust on the IoT devices among the users [44]. It is suggested that the connected networks must have good intentions between them and must be transparent in all inter communications [45].

Apart from the security and network challenges, there are also software development challenges where new software must be integrated along with the existing software. Concepts like big data make a huge impact since it cannot be implemented in existing systems and require a huge infrastructure. IoT also requires humans to be in the loop since not everything can be automated at this stage.

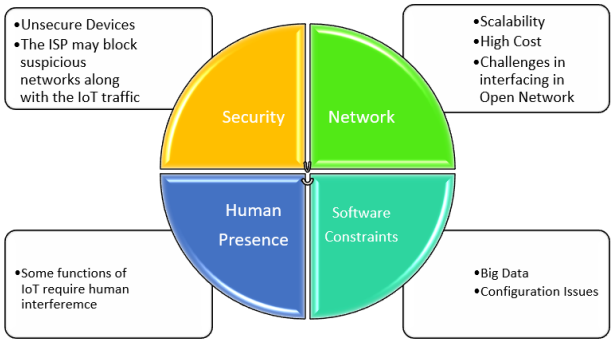

Figure 2: Challenges in IoT Network

3. Ransomware

A ransomware is a type of malware that takes control of a system or data and restricts access to the devices for the user. A large amount is demanded as ransom and the data is released only after the payment is successful. The attacker may threaten to delete the data permanently if the user refuses to pay the amount [46]. Contrary to conventional threats, ransomware may be more dangerous since the entire parameters of the services like the availability, integrity and confidentiality is affected,, which may lead to a financial or information loss [47]. Its preliminary version appeared in 1989 and was known as Aids info disk. It spread through floppy disks and kept track on the number of times a system was restarted. It got active once it is restarted 90 times [48]. The files in the C directory either got encrypted or hidden. However, it couldn't spread to large areas since the computer network were not as much connected as they are today. The same technique was used in the malware that appeared later, but started to demand a ransom for reversing the effects. They spread through fake applications, insecure websites, etc [49]. These applications trick the users that the system is in danger and make them to download fake applications thereby activating the malware.

The number of attacks are growing exponentially since earlier computers were not well connected and hence the attackers faced difficulties getting money from the users. However, the advent of crypto currencies like Bitcoin has made it easier for the attackers to demand money from the users anonymously. The large growth of IoT devices and its inter-connectivity to the network has enabled the increase in ransomware. The attack works different for devices with and without displays [50, 51]. The hackers initially gain access to the devices, encrypt the files and then demand the ransom for unlocking the devices [52]. This is however difficult in IoT devices since it is challenging for the attackers to find the owners of devices. Most of the devices are controlled by other devices and hence it is difficult to tracks the hierarchy. The attacks take place only if the attacker identifies the hierarchy in the network. Smaller devices have not been attacked regularly since they are insignificant to the attackers and the users may not pay the ransom. While conventional ransomware attacks can be done from a single server, attacks on IoT devices may be required from multiple systems and devices [53]. There are three types of ransomware

- Crypto

Retrieval Number: I33090789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3309.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

- Locker
- Hybrid

3.1 Crypto Ransomware

This type of ransomware encrypts the data in the devices and asks for ransom. Once the ransom is paid, a key is then provided form decrypting the data. This is the most commonly used type of ransomware due to its ability to induce lots of damage [54]. It works on a different keys combination where the encryption and decryption is done using keys which is provided on paying the ransom. It is more dangerous for IoT devices, where the back end servers are attacked since they have lots of data [55]. The most popular crypto ransomware is TeslaCrypt which is considered to be responsible for 58.43% of all the ransomware attacks. It can attack multiple devices simultaneously making it a large threat to the IoT users. The crypto Ransomware may be categorised into two types based on the type of encryption.

3.1.1 Symmetric Crypto-Ransomware

It is a type of crypto-ransomware that utilizes a single private key for both encryption and decryption. Different types of encryption techniques may be applied like the Data Encryption Standard (DES), Rivest Cipher 4 (RC4), Advanced Encryption Standard (AES), etc. [56]. As the name suggests, the same key is used for both encryption and decryption. However, this makes it weaker since sharing the same key leads to disclosure [57].

3.1.2 Asymmetric Crypto-Ransomware

It is a type of Crypto ransomware where different sets of keys are used for encryption and decryption. While the public key is used for encryption, a private key may be utilized for decryption [58]. Hence, it can easily withstand any tampering attempts. It works on a public – private keys combination where the encryption is performed with public keys since the same set of keys may be used for encrypting multiple devices. The decryption is done using private keys which is provided on paying the ransom. [59].

3.2 Locker Ransomware

While the crypto ransomware encrypts the data in plain sight, the locker ransomware hides the data rendering them invisible to the user. They might even alter the functionality of the IoT devices making them work in other ways then they are intended to [59]. They might even complete shut down the device thereby disabling them. This may create problems for the users or the organisation leading to losses. When the ransom is paid and the data is restored, the files remain intact and the IoT devices start to work similar to its original functions. Hence, it is not very effective and it is not used as widely as crypto Ransomware [60]. When both these major ransomware are given, crypto ransomware constitute around 64% of the total attacks while locker ransomware constitute the remaining 36%.

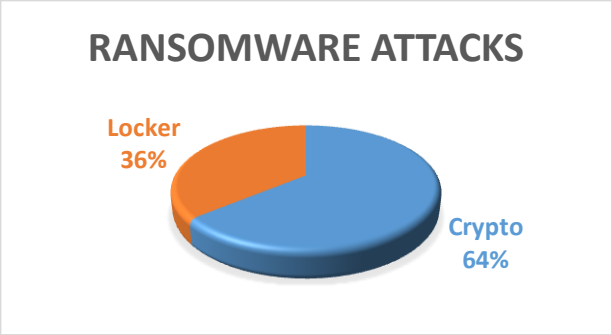

Figure 3: Challenges in IoT Network

3.3 Hybrid Ransomware

This type of ransomware combines the functionalities of both crypto ransomware and locker ransomware. They are more dangerous than both of the individual types since both the data and functionality gets compromised [59]. It targets both the front end and back end of the devices and is very dangerous for IoT devices. However, launching such an attack on IoT devices is difficult since it is challenging for such a type to penetrate the multiple layers in the heterogeneous system. But if the attackers are successful in launching them, then the whole network may get damaged.

4 Spread of Ransomware

Ransomware like other malware have lots of different ways of reaching their destination. Since the security systems are getting improved and taking measures to stop the malware, the attackers find different methods and loopholes to maintain their spread. Since reaching the IoT devices is difficult, there are not many ways for the ransomware to reach these devices. However, the following methods have been successful in delivering the ransomware to the IoT devices.

4.1 Phishing and Botnets

Phishing mails are common where the attackers camouflage their links as a legitimate service like banks in order to click on a link. Phishing utilises social engineering methods where the attackers portray themselves as other legal authorities for collecting the data. This will enable botnets to enter an IoT network attached to other files and get activated, thereby compromising the entire network. Botnets are a tool for the Distributed Denial of Service (DDoS), where the attacks may enter from multiple location at a same time with the help of botnets [61]. It is difficult to secure the network once it gets compromised since the data and network hierarchy of the device is known to the attacker and may even

Retrieval Number: I33090789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3309.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

share the details with other attackers and botnet administrators. Hence, once compromised the network remains as such for a long time even after getting rid of the prevailing ransomware.

4.2 False Advertising

Lots of ransomware freely moves in general traffic attached to other multimedia content [62]. The attackers can place the malware in the traffic that is designated to a certain user in both the back end and the front end devices. False advertising a certain product makes the user install it into the IoT system where the ransomware gets installed thereby compromising the network. This is dangerous for both security and privacy and can be avoided if the users are careful to install only materials only from trusted sources.

4.3 Software-as-a-Service (SaaS)

IoT devices and network depend very much on the cloud services to get the necessary data and directions. When ransomware intercepts a particular SaaS and compromise it, it enters the IoT network when it avails this service. Initially, it might seem like legitimate content, however, after getting installed, it spreads quickly inside the network to all levels it has access to.

5 Case Studies

Since the IoT network is a fairly new concept, there are not lot of ransomware attacks for IoT reviewed in the literature. Some case studies and possibilities of Ransomware in IoT are given below.

5.1 Smart Vehicles

The ordinary commercial cars have some kind of connectivity with the internet in the recent times. Most cars now have some kind of operating systems making them a perspective IoT device. Hence, they are susceptible to Ransomware attacks when they are connected to the internet. Most of these units never receive an upgrade from the manufacturer and hence they cannot resist the attacks from the network attacks.

A ransomware attack on the car can be dangerous especially on self-driving cars since they have the ability to control your steering. The attacker can effectively lock your car and demand a payment or even lock the steering wheel for the ransom. This can cause a severe harm and put the life of the user in danger, since the attackers will be able to take control of the car while driving. The attackers may start driving your car and steer it away from the traffic into deserted places.

This brings problems economically as well. Larger connected vehicles that transport goods may get compromised and taken control bringing financial loses since the cargo has to reach on time. This forces the owner to pay the ransom very quickly since it will take a lot of time to take any counter measures. The potential harm is high and there are lots of other possibilities to the connected vehicles.

5.2 Smart Homes

The number of smart homes are increasing day by day in developed nations. The smart devices in homes can be controlled remotely from anywhere in the world through the internet. The houses can be locked and unlocked, devices can be turned on and off remotely. However, these advantages bring an enormous disadvantage, where the hackers will also be able to gain access and control the devices in the homes. They can increase the usage of our electricity bills and even lock the houses denying entry or exit from the homes.

This a huge opportunity for ransomware since a huge ransom may be demanded for letting the person outside the homes. There are also chances of repeated attacks since the attacker will prospectively know the way around the network and may repeat the process again, thereby repeatedly demanding the ransoms.

5.3 Medical Equipment

The medical industry is experiencing a drastic change with the introduction of IoT devices. These devices are used for diagnosing various devices and also keeping a person alive. The devices may be controlled over the internet so that the doctor or a medical representative may keep an eye on chronic patients even when they are at home. Bed ridden patients may even be controlled by the doctors by regulating the supply of oxygen, etc.

However, when this technology falls in the hands of the hackers, they use this opportunity to induce ransomwares thereby gaining control of the equipment. This pts the life of the patients at risk since they can project false information to the doctors and also simultaneously weaken the patients' health. The attacks on these live saving supports and other devices like MRI poses a serious threat for the IoT network.

Since these devices are interconnected to each other in the hospitals either through wired or wireless connections, the infection can spread to other devices thereby allowing the other devices to succumb under the hackers' control. With this, the entire network gets compromised thereby increasing the ransom amount multiple fold. This puts the processes at the hospital in a serious trouble and puts the hackers in an advantageous position.

5.4Wearable Devices

The number of wearable devices have been increasing recently and are an easy target since the security features are

Retrieval Number: I33090789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3309.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

minimal. There is even an unofficial term "Ransomwear" to talk about this. However, these attacks are not a major threat since the data stored in these devices and its applications are minimal. Since the users are not entirely dependent on them, the ransomware attack on the devices does not have much consequence.

An attack on the device may lead to loss of some minimal data. Resetting the device can remove the threat. Hence, the attackers usually demand a very small amount so that the users will be ready to pay the amount rather than resetting them and losing their data. It will not be profitable for the hackers to demand a huge sum since that would not be profitable.

However, the attackers may infect a huge number if devices at the same time and extort the money so that even if 25% of them pay, they will be able to make a profit out of the attack.

6 Combatting Ransomware

The attacks can be reduced to a certain extent by ensuring certain checklists. Since every attack is different, there is no single way of mitigating the attacks. Hence, the entire network must be scanned regularly for any signs of malware or attacks. The users must also be trained to periodically switch off the devices and upgrading the necessary firmware provided by the company. Other defence strategies may be used where the ransomware may be scanned at individual levels and layers [63, 64]. In spite of these security measures, the attackers enter the systems with some other bugs or loop-holes or even carelessness by the users. If this happens, the damages must be reversed as quickly as possible by the following methods.

- A team of experts must be engaged to remove the ransomware or to mitigate the damages that may take place in the IoT network. The devices must be switched off and efforts should be made to remove the infection from the network. An alternative device may be connected in place of the affected system to ensure disruption of service.

- While not everyone may have the resources and affordability to hire experts, the users must have basic knowledge on handling these threats. The users must use a reliable security software to stop these attacks and enhance the security in the system.

- Since the data is main factor targeted by the attackers, it must be regularly backed up by the users to other servers. This may provide efficient replacement of data even if it gets deleted by the ransomware. If the data is backed up securely, the users do not need to worry about spending money on paying the ransom amount since their data is safe and can be transferred elsewhere.

The challenges in the security of IoT arises due to rapid rise and the sheer number of devices that are interconnected [65]. Some of the challenges may arise during mitigation and combatting ransomware:

- The Ransomware cannot be combatted simply by switching off the devices in most of the times since the data has already been compromised and the users do not have any other alternative.

- The users also should not download certain types of files and only download those that are absolutely necessary. The device manufacturers may provide a list of predefined file types thereby educating the user on the type of files that is necessary and those that can be considered to be safe.

- Since the network and the devices are highly heterogeneous, there are limitations in bringing a uniformity to the design. The security protocols must be designed specifically for individual types of ransomware. Hence, new emerging attacks go undetected till the firmware is upgraded to detect the new ones.

7 Related Work

Security is the major aim in different domains like wireless sensors and networks [66, 67], however, it is still not completely developed in case of IoT networks. A secure technique known as Authenticated Publish Subscribe (AUPS) has been proposed by Rizzardi et al.[68] by extending the existing IoT protocol. A secure subscription system has been introduced within the protocol with a novel key management technique, thereby controlling the data flow in the system more efficiently. A novel security framework has been proposed by Tao et al [69] for providing better services in IoT enabled smart homes through cloud models. This allows better flow of information between devices of different manufacturers. However, the proposed model has not been completely developed to meet the security standards of live IoT networks. A thorough security solution is proposed by Moosavi et al. [70] for securing a IoT based healthcare system. A Datagram TLS has been utilised between the users along with the ability to resume the sessions. The proposed model works efficiently than the existing models on the metrics of energy consumption, throughput and latency. However, the energy consumption is not as per the standards and consumes a lot.

A distributed middleware layer system has been developed by Sicari et al., [71], where the heterogeneous data may be managed and its security may be evaluated. The trustworthiness of the IoT data can be measured and assessed. Integration of a key management system is proposed as a future scope in this research. Perumal et al. [72] has proposed a model to help the forensic investigators in IoT networks. It works on the basis of multilayer model in volatile based data preservation. Even though the proposed technique may help the forensic investigators, it is still difficult to conduct in practical live IoT networks. Security related problems of

Retrieval Number: I33090789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3309.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

wearable IoT devices have been investigated by comparing the production techniques of the manufacturers with respect to security and privacy [73]. An automatic authentication system for identifying and recognising the forgery is audio devices is performed in some devices [74, 75].

Sundaram et al., [76] have attempted to improve the security in IoT systems in smart homes. In case of an attack, the data may get lost using SQL injection and then the OS might get corrupted. An encryption based hash algorithm has been proposed so that the IoT devices like thermostat and door controls may communicate securely. Santos et al. [77] has stressed on improving the security while communication between the IoT devices. To find a way out of the different issues, an architecture has been framed which allows the IoT devices to utilise DTLS where the authentication takes place mutually. Similarly, Alcon et al., [78] has proposed a technique to calculate the secureness of the IoT system for different devices. However, it was tested on a modal and not in real time applications.

Small IoT devices uses different key sharing protocols like PSK or RPK. They require implementing individual objects for each users of IoT. This is difficult for large number of objects. This has been addressed by Raza et al.[79] by proposing a novel key based architecture known as S3K. With this method, large number of IoT objects can communicate with each other. Hernandez-Ramos et al., [80] has proposed a novel IoT architecture for implementing necessary privacy and security measures for the IoT devices throughout their lifetime. The recommended architectural design in this research is based on the design of diverse security and privacy mechanisms.

8 Scope for future research

There is a huge scope of research in the security of IoT devices since the concept in still in development stage. Since ransomware can enter into the network through any security lapse, it should be ensured that the security is increased through extensive research and development.

There are problems associated with third party applications in the IoT devices. Some of these applications may seek more access than what is required for its working [81]. Ransomware can enter the devices through these unauthorised applications lead to the complications. It is difficult to control these applications since some of them do not do so intentionally, but they are compromised without their knowledge. This is partly due to presence of large number of connected devices [82, 83]. These applications get exploited to install dangerous codes [84]. The various threats work differently for inducing the malfunctioning of devices. There are several reason to these applications getting compromised. The main reason is that the devices are not able to receive any security patches [85]. Hence, this should be enhanced to avoid and deter any type of attacks on the network especially ransomware attacks, thereby providing a great opportunity for research in the future research.

Attack of IoT sensors are another target for the attackers. They change the perception of data that is received from the sensors leading to malfunctioning of the device. They can also make the device to altogether stop working and demand a ransom for allowing the sensors to work [86]. These threats come from outside the entities usually with the context of gathering information. As the IoT is susceptible to different types of attacks, there are lots of security problems. Ransomware is not the sole threat that must be addressed. Future research can be undertaken for improving the network against all the known attacks.

The network is susceptible to noisy data since having large amount data leads to congestion in the network [87]. Most of the threats arises from the gap in authentication and integrity. Some of the most common attacks other than ransomware are Denial of Service (DoS) attack [88], Unapproved Access of data and gateway attacks [89]. The network can get compromised while transmitting the data leading to problems. Research on preventing these attacks has a huge scope for research in the future. Another scope for research is security of sensors and actuators. Since physical protection cannot be provided for the sensors located in remote locations, more energy efficient devices can be researched in the future.

9. Conclusion

There are a plethora of advancements in the smart technologies that have paved the way for smarter and novel techniques in the field of IoT. This is evident especially for security features to mitigate the network attacks like Ransomware. This chapter has studied the IoT network and the challenges faced in the network. Security has been pointed out the major issue in IoT devices and different attacks are discussed. Ransomware, the major concern of this chapter is discussed, and its types are studied.

The Ransomware in IoT devices are especially concentrated upon and the problems faced in mitigating them in IoT devices and network has been provided. Also, case studies that concern the Ransomwares in IoT devices are studied. Finally, different major research directions are given for the researchers in future. It has been conveyed that there is a major scope in the future for research since the development and security are still in the infant stage for IoT network. It has been pointed out that the IoT devices are very vulnerable to ransomware attacks. Hence, it is necessary to strengthen the security in the network in order to mitigate the different attacks, especially ransomware.

REFERENCES

1. Tobias RJ. Wireless communication of real-time ultrasound data and control. In: In SPIE Medical Imaging International Society for Optics and Photonics [Internet]. SPIE; 2015. Available from: http://sci-hub.tw/10.1016/j.comnet.2017.09.003
2. Ahmed E, Yaqoob I, Gani A, Imran M, Guizani M. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. IEEE Wirel Commun. 2016 Oct;23(5):10–6.
3. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun Surv Tutorials. 2015;17(4):2347–76.

Retrieval Number: I33090789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3309.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

4. Lin D, Tang Y, Labeau F, Yao Y, Imran M, Vasilakos A V. Internet of Vehicles for E-Health Applications: A Potential Game for Optimal Network Capacity. IEEE Syst J [Internet]. 2017 Sep;11(3):1888–96. Available from: http://ieeexplore.ieee.org/document/7174983/

5. Ghosh AM, Halder D, Hossain SKA. Remote health monitoring system through IoT. In: 2016 5th International Conference on Informatics, Electronics and Vision (ICIEV) [Internet]. IEEE; 2016. p. 921–6. Available from: http://ieeexplore.ieee.org/document/7760135/

6. Khoi NM, Saguna S, Mitra K, Ahlund C. IReHMo: An efficient IoT-based remote health monitoring system for smart regions. In: 2015 17th International Conference on E-health Networking, Application & Services (HealthCom) [Internet]. IEEE; 2015. p. 563–8. Available from: http://ieeexplore.ieee.org/document/7454565/

7. Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context Aware Computing for The Internet of Things: A Survey. IEEE Commun Surv Tutorials [Internet]. 2014;16(1):414–54. Available from: http://ieeexplore.ieee.org/document/6512846/

8. Sanduleac M, Chimirel CL, Eremia M, Toma L, Cristian C, Stanescu D. Unleashing Smart Cities efficient and sustainable energy policies with IoT based Unbundled Smart Meters. In: 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech) [Internet]. IEEE; 2016. p. 112–7. Available from: http://ieeexplore.ieee.org/document/7737321/

9. Yaqoob I, Ahmed E, Rehman MH ur, Ahmed AIA, Al-garadi MA, Imran M, et al. The rise of ransomware and emerging security challenges in the Internet of Things. Comput Networks [Internet]. 2017 Dec 24 [cited 2019 May 1];129:444–58. Available from: https://www.sciencedirect.com/science/article/abs/pii/S1389128617303468

10. Wamala F. The ITU National Cybersecurity Strategy Guide [Internet]. ITU. 2011 [cited 2018 May 3]. Available from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

11. Jain K. These Top 7 Brutal Cyber Attacks Prove "No One is Immune to Hacking" [Internet]. The Hacker News. 2015 [cited 2018 May 3]. Available from: https://thehackernews.com/2015/09/top-cyber-attacks-1.html

12. Lohrmann D. 2015: The Year Data Breaches Became Intimate [Internet]. Govtech. 2015 [cited 2019 May 3]. Available from: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2015-the-year-data-breaches-became-intimate.html

13. ENISA. ENISA Threat Landscape 2015 [Internet]. 2016 [cited 2019 May 3]. Available from: https://www.enisa.europa.eu/publications/etl2015

14. Jing Q, Vasilakos A V., Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. Wirel Networks [Internet]. 2014 Nov 17;20(8):2481–501. Available from: http://link.springer.com/10.1007/s11276-014-0761-7

15. Pacheco J, Satam S, Hariri S, Grijalva C, Berkenbrock H. IoT Security Development Framework for building trustworthy Smart car services. In: 2016 IEEE Conference on Intelligence and Security Informatics (ISI) [Internet]. IEEE; 2016. p. 237–42. Available from: http://ieeexplore.ieee.org/document/7745481/

16. Wen Q, Dong X, Zhang R. Application of dynamic variable cipher security certificate in Internet of Things. In: 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems [Internet]. IEEE; 2012. p. 1062–6. Available from: http://ieeexplore.ieee.org/document/6664544/

17. Ketema G, Hoebeke J, Moerman I, Demeester P, Tao LS, Jara AJ. Efficiently Observing Internet of Things Resources. In: 2012 IEEE International Conference on Green Computing and Communications [Internet]. IEEE; 2012. p. 446–9. Available from: http://ieeexplore.ieee.org/document/6468349/

18. Granjal J, Monteiro E, Sa Silva J. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Commun Surv Tutorials [Internet]. 2015;17(3):1294–312. Available from: http://ieeexplore.ieee.org/document/7005393/

19. Zhao K, Ge L. A Survey on the Internet of Things Security. In: 2013 Ninth International Conference on Computational Intelligence and Security [Internet]. IEEE; 2013. p. 663–7. Available from: http://ieeexplore.ieee.org/document/6746513/

20. Yan Z, Zhang P, Vasilakos A V. A survey on trust management for Internet of Things. J Netw Comput Appl [Internet]. 2014 Jun;42:120–34. Available from: https://linkinghub.elsevier.com/retrieve/pii/S1084804514000575

21. Alaba FA, Othman M, Hashem IAT, Alotaibi F. Internet of Things security: A survey. J Netw Comput Appl [Internet]. 2017 Jun;88:10–28. Available from: https://linkinghub.elsevier.com/retrieve/pii/S1084804517301455

22. Weber RH. Internet of Things – New security and privacy challenges. Comput Law Secur Rev [Internet]. 2010 Jan;26(1):23–30. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0267364909001939

23. Suo H, Wan J, Zou C, Liu J. Security in the Internet of Things: A Review. In: 2012 International Conference on Computer Science and Electronics Engineering [Internet]. IEEE; 2012. p. 648–51. Available from: http://ieeexplore.ieee.org/document/6188257/

24. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. Comput Networks. 2013 Jul;57(10):2266–79.

25. Kumar JS, Patel DR. A Survey on Internet of Things: Security and Privacy Issues. Int J Comput Appl [Internet]. 2014 Mar 26;90(11):20–6. Available from: http://research.ijcaonline.org/volume90/number11/pxc3894454.pdf

26. Bertino E, Islam N. Botnets and Internet of Things Security. Computer (Long Beach Calif) [Internet]. 2017 Feb;50(2):76–9. Available from: http://ieeexplore.ieee.org/document/7842850/

27. Chen L, Thombre S, Jarvinen K, Lohan ES, Alen-Savikko A, Leppakoski H, et al. Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey. IEEE Access [Internet]. 2017;5:8956–77. Available from: http://ieeexplore.ieee.org/document/7903611/

28. Bradshaw S. Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity [Internet]. GCIG. 2015 [cited 2019 May 3]. Available from: https://www.cigionline.org/publications/combatting-cyber-threats-csirts-and-fostering-international-cooperation-cybersecurity

29. Donston-Miller D. The Internet Of Things Poses New Security Challenges [Internet]. Forbes. 2014 [cited 2019 May 3]. Available from: https://www.forbes.com/sites/sungardas/2014/02/25/the-internet-of-things-poses-new-security-challenges/#276cf9062c6f

30. Davis G. Brace Yourselves: The 'Perfect Security Storm' is Coming [Internet]. 2015 [cited 2019 May 3]. Available from: https://sci-hub.tw/10.1016/j.clsr.2016.07.002

31. Rezendes CJ, Stephenson WD. Cyber Security in the Internet of Things. 2013.

32. Lee J-H, Kim H. Security and privacy challenges in the internet of things [security and privacy matters]. IEEE Consum Electron Mag [Internet]. 2017;6(3):134– 136. Available from: https://sci-hub.tw/10.1016/j.comnet.2017.09.003

33. Liu C, Yang C, Zhang X, Chen J. External integrity verification for outsourced big data in cloud and IoT: A big picture. Futur Gener Comput Syst. 2015 Aug;49:58–67.

34. Gao M, Wang Q, Arafin MT, Lyu Y, Qu G. Approximate computing for low power and security in the internet of things. Computer (Long Beach Calif) [Internet]. 2017;50(6):27–34. Available from:

Retrieval Number: I33090789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3309.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

https://ieeexplore.ieee.org/document/7945174

35. Salami S Al, Baek J, Salah K, Damiani E. Lightweight encryption for smart home," in Availability, Reliability and Security (ARES). In: 2016 11th International Conference on [Internet]. IEEE; 2016. p. 382–388. Available from: https://ieeexplore.ieee.org/document/7784596

36. Raza S, Shafagh H, Hewage K, Hummen R, Voigt T. Lithe: Lightweight Secure CoAP for the Internet of Things. IEEE Sens J [Internet]. 2013 Oct;13(10):3711–20. Available from: http://ieeexplore.ieee.org/document/6576185/

37. Challa S, Wazid M, Das AK, Kumar N, Reddy AG, Yoon E-J, et al. Secure signature-based authenticated key establishment scheme for future iot applications. IEEE Access [Internet]. 2017;5:3028–3043. Available from: https://sci-hub.tw/10.1016/j.comnet.2017.09.003

38. Ko H, Jin J, Keoh SL. Secure service virtualization in iot by dynamic service dependency verification. IEEE Internet Things J [Internet]. 2016;3(6):1006–1014. Available from: https://ieeexplore.ieee.org/document/7439733

39. Cheng C, Lu R, Petzoldt A, Takagi T. Securing the internet of things in a quantum world. IEEE Commun Mag [Internet]. 2017;55(2):116–120. Available from: https://sci-hub.tw/10.1016/j.comnet.2017.09.003

40. Alkeem E Al, Yeun CY, Zemerly MJ. Security and privacy framework for ubiquitous healthcare IoT devices. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) [Internet]. London, UK: IEEE; 2016. Available from: https://ieeexplore.ieee.org/document/7412059

41. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in internet of things: The road ahead. Comput Networks [Internet]. 2015;76:146–164. Available from: https://www.sciencedirect.com/science/article/abs/pii/S1389128614003971

42. Tian C, Chen X, Guo D, Sun J, Liu L, Hong J. Analysis and design of security in internet of things. In: In 2015 8th International Conference on Biomedical Engineering and Informatics (BMEI) [Internet]. Shenyang, China: IEEE; 2015. p. 678–684. Available from: https://ieeexplore.ieee.org/document/7401589

43. Premnath SN, Haas ZJ. Security and privacy in the internet-of-things under time-and-budget-limited adversary model. IEEE Wirel Commun Lett [Internet]. 2015;4(3):277–280. Available from: https://ieeexplore.ieee.org/document/7054433

44. Chen R, Bao F, Guo J. Trust-based service management for social internet of things systems. IEEE Trans Dependable Secur Comput [Internet]. 2016;13(6):684–696. Available from: https://ieeexplore.ieee.org/document/7097037

45. Gu L, Jingpei W, Bin S. Trust management mechanism for internet of things. China Commun [Internet]. 2014;11(2):148–156. Available from: https://ieeexplore.ieee.org/document/6821746

46. Nassi B, Shamir A, Elovici Y. Oops!... i think i scanned a malware [Internet]. 2017 [cited 2018 May 3]. Available from: https://www.semanticscholar.org/paper/Oops!...I-think-I-scanned-a-malware-Nassi-Shamir/ee538c0da7709c8d376749e74fc2451c70fb8d90

47. Bertino E, Islam N. Botnets and Internet of Things Security. Computer (Long Beach Calif). 2017 Feb;50(2):76–9.

48. Richardson R, North M. Ransomware: Evolution, mitigation and prevention. Int Manag Rev [Internet]. 2017;13(1):10–21. Available from: http://scholarspress.us/journals/IMR/pdf/IMR-1-2017. pdf/IMR-v13n1art2.pdf

49. Bugeja J, Jacobsson A, Davidsson P. An analysis of malicious threat agents for the smart connected home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) [Internet]. IEEE; 2017. p. 557–62. Available from: https://ieeexplore.ieee.org/document/7917623/

50. Kavya D. Ransomware of things (rot). Fuzzy Syst [Internet]. 2017;9(2):29–32. Available from: http://sci-hub.tw/10.1016/j.comnet.2017.09.003

51. Adat V, Gupta BB. Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommun Syst [Internet]. 2018 Mar 13;67(3):423–41. Available from: http://link.springer.com/10.1007/s11235-017-0345-9

52. D'Orazio CJ, Choo K-KR, Yang LT. Data Exfiltration From Internet of Things Devices: iOS Devices as Case Studies. IEEE Internet Things J [Internet]. 2017 Apr;4(2):524–35. Available from: http://ieeexplore.ieee.org/document/7470257/

53. Ring T. Connected cars–the next target for hackers. Netw Secur [Internet]. 2015;(11):11–16. Available from: http://sci-hub.tw/10.1016/j.comnet.2017.09.003

54. Gostev A, Unuchek R, Garnaeva M, Makrushin D, Ivanov A. IT Threat Evolution in Q1 2016 [Internet]. Kaspersky Lab. 2016 [cited 2019 May 23]. Available from: https://securelist.com/it-threat-evolution-in-q1-2016/74640/

55. Gonzalez D, Hayajneh T. Detection and prevention of crypto-ransomware. In: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) [Internet]. IEEE; 2017. p. 472–8. Available from: http://ieeexplore.ieee.org/document/8249052/

56. Kong JH, Ang L-M, Seng KP. A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments. J Netw Comput Appl [Internet]. 2015;49:15–50. Available from: https://www.sciencedirect.com/science/article/pii/S1084804514002136?via%3Dihub

57. Shim KA. A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks. IEEE Commun Surv Tutorials [Internet]. 2016;18(1):577–601. Available from: https://sci-hub.se/https%3A%2F%2Fwww.sciencedirect.com%2Fscience%2Farticle%2Fpii%2FS016740481830004X

58. Ahmadian MM, Shahriari HR, Ghaffarian SM. Connection-monitor and connection-breaker: A novel approach for prevention and detection of high survivable ransomwares. In: Paper presented at the 12th International ISC Conference on Information Security and Cryptology, ISCISC 2015 [Internet]. 2015. p. 79–84. Available from: https://sci-hub.se/https%3A%2F%2Fwww.sciencedirect.com%2Fscience%2Farticle%2Fpii%2FS016740481830004X

59. Al-rimy BAS, Maarof MA, Shaid SZM. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Comput Secur [Internet]. 2018 May;74:144–66. Available from: https://linkinghub.elsevier.com/retrieve/pii/S016740481830004X

60. Savage K, Coogan P, Lau H. The evolution of ransomware [Internet]. 2015 [cited 2019 May 18]. Available from: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

61. Cheng S-M, Chen P-Y, Lin C-C, Hsiao H-C. Traffic-Aware Patching for Cyber Security in Mobile IoT. IEEE Commun Mag [Internet]. 2017;55(7):29–35. Available from: http://ieeexplore.ieee.org/document/7981520/

62. Cabaj K, Gregorczyk M, Mazurczyk W. Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. Comput Electr Eng [Internet]. 2018 Feb;66:353–68. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0045790617333542

63. Castilho SD, Godoy EP, Castilho TWL, Salmen AF. Proposed model to implement high-level Information Security in Internet of Things. In: 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC) [Internet]. IEEE; 2017. p. 165–70. Available from: http://ieeexplore.ieee.org/document/7946425/

64. Stewart CE, Vasu AM, Keller E. Communityguard: A crowdsourced home cyber-security system. In: Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization - SDN-NFVSec '17 [Internet]. New York, New York, USA: ACM Press; 2017. p. 1–6.

Retrieval Number: I33090789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3309.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Available from: http://dl.acm.org/citation.cfm?doid=3040992.3040997

65. Solangi ZA, Solangi YA, Chandio S, bt. S. Abd. Aziz M, bin Hamzah MS, Shah A. The future of data privacy and security concerns in Internet of Things. In: 2018 IEEE International Conference on Innovative Research and Development (ICIRD) [Internet]. IEEE; 2018. p. 1–4. Available from: https://ieeexplore.ieee.org/document/8376320/
66. Hayajneh T, Mohd B, Imran M, Almashaqbeh G, Vasilakos A. Secure Authentication for Remote Patient Monitoring with Wireless Medical Sensor Networks. Sensors [Internet]. 2016 Mar 24;16(4):424. Available from: http://www.mdpi.com/1424-8220/16/4/424
67. Shu Z, Wan J, Li D, Lin J, Vasilakos A V., Imran M. Security in Software-Defined Networking: Threats and Countermeasures. Mob Networks Appl [Internet]. 2016 Oct 12;21(5):764–76. Available from: http://link.springer.com/10.1007/s11036-016-0676-x
68. Rizzardi A, Sicari S, Miorandi D, Coen-Porisini A. AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things. Inf Syst [Internet]. 2016 Dec;62:29–41. Available from: http://linkinghub.elsevier.com/retrieve/pii/S030643791630237X
69. Tao M, Zuo J, Liu Z, Castiglione A, Palmieri F. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Futur Gener Comput Syst [Internet]. 2018 Jan;78:1040–51. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0167739X16305775
70. Moosavi SR, Gia TN, Nigussie E, Rahmani AM, Virtanen S, Tenhunen H, et al. End-to-end security scheme for mobility enabled healthcare Internet of Things. Futur Gener Comput Syst [Internet]. 2016 Nov;64:108–24. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0167739X16300334
71. Sicari S, Rizzardi A, Miorandi D, Cappiello C, Coen-Porisini A. A secure and quality-aware prototypical architecture for the Internet of Things. Inf Syst [Internet]. 2016 Jun;58:43–55. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0306437916300072
72. Perumal S, Norwawi NM, Raman V. Internet of Things(IoT) digital forensic investigation model: Top-down forensic approach methodology. In: 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC) [Internet]. IEEE; 2015. p. 19–23. Available from: http://ieeexplore.ieee.org/document/7323000/
73. Arias O, Wurm J, Hoang K, Jin Y. Privacy and Security in Internet of Things and Wearable Devices. IEEE Trans Multi-Scale Comput Syst [Internet]. 2015 Apr 1;1(2):99–109. Available from: http://ieeexplore.ieee.org/document/7321811/
74. Ali Z, Imran M, Alsulaiman M. An Automatic Digital Audio Authentication/Forensics System. IEEE Access [Internet]. 2017;5:2994–3007. Available from: http://ieeexplore.ieee.org/document/7864411/
75. Imran M, Ali Z, Bakhsh ST, Akram S. Blind Detection of Copy-Move Forgery in Digital Audio Forensics. IEEE Access [Internet]. 2017;5:12843–55. Available from: http://ieeexplore.ieee.org/document/7954589/
76. Sundaram BV, Ramnath M, Prasanth M, Sundaram VJ. Encryption and hash based security in Internet of Things. In: 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN) [Internet]. IEEE; 2015. p. 1–6. Available from: http://ieeexplore.ieee.org/document/7219926/
77. Santos GL dos, Guimaraes VT, da Cunha Rodrigues G, Granville LZ, Tarouco LMR. A DTLS-based security architecture for the Internet of Things. In: 2015 IEEE Symposium on Computers and Communication (ISCC) [Internet]. IEEE; 2015. p. 809–15. Available from: http://ieeexplore.ieee.org/document/7405613/
78. Alcon J-AS, Lopez L, Martinez J-F, Castillejo P. Automated determination of security services to ensure personal data protection in the Internet of Things applications. In: Third International Conference on Innovative Computing Technology (INTECH 2013) [Internet]. IEEE; 2013. p. 71–6. Available from: http://ieeexplore.ieee.org/document/6653704/
79. Raza S, Seitz L, Sitenkov D, Selander G. S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the Internet of Things. IEEE Trans Autom Sci Eng [Internet]. 2016 Jul;13(3):1270–80. Available from: http://ieeexplore.ieee.org/document/7373695/
80. Hernandez-Ramos JL, Bernabe JB, Skarmeta A. ARMY: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things. IEEE Commun Mag [Internet]. 2016 Sep;54(9):28–35. Available from: http://ieeexplore.ieee.org/document/7565269/
81. Kolias C, Stavrou A, Voas J, Bojanova I, Kuhn R. Learning internet-of-things security hands-on. IEEE Secur Priv [Internet]. 2016;14(1):37–46. Available from: https://ieeexplore.ieee.org/document/7397713
82. Xiaohui X. Study on security problems and key technologies of the internet of things. In: In Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on [Internet]. Shiyang, China: IEEE; 2013. p. 407–410. Available from: https://ieeexplore.ieee.org/document/6643029
83. Kozlov D, Veijalainen J, Ali Y. Security and privacy threats in iot architectures. In: In Proceedings of the 7th International Conference on Body Area Networks [Internet]. Oslo: ICST; 2012. p. 256–262. Available from: https://dl.acm.org/citation.cfm?id=2442750
84. Ning H, Liu H, Yang LT. Cyberentity security in the internet of things. Computer (Long Beach Calif) [Internet]. 2013;46(4):46–53. Available from: https://ieeexplore.ieee.org/document/6475947
85. Kim D-Y. Cyber security issues imposed on nuclear power plants. Ann Nucl Energy [Internet]. 2014;65:141– 143. Available from: https://www.sciencedirect.com/science/article/pii/S0306454913005781
86. Li S, Xu L Da, Zhao S. The internet of things: a survey. Inf Syst Front [Internet]. 2015;17(2):243. Available from: https://link.springer.com/article/10.1007/s10796-014-9492-7
87. Bostani H, Sheikhan M. Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach. Comput Commun [Internet]. 2017 Jan;98:52–71. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0140366416306387
88. Savola RM, Abie H, Sihvonen M. Towards metrics-driven adaptive security management in e-health iot applications. In: In Proceedings of the 7th International Conference on Body Area Networks ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012 [Internet]. ICST; 2012. p. 276–281. Available from: https://dl.acm.org/citation.cfm?id=2442753
89. Kanuparthi A, Karri R, Addepalli S. Hardware and embedded security in the context of internet of things. In: In Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles [Internet]. M New York: ACM; 2013. p. 61–64. Available from: https://dl.acm.org/citation.cfm?id=2517976

Retrieval Number: I33090789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3309.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication