An Overview on Security Issues In Internet Of Things

Mohammad Luqman
Department of Computer Science
Aligarh Muslim University
Aligarh, India
luqman.geeky@gmail.com

Arman Rasool Faridi
Department of Computer Science
Aligarh Muslim University
Aligarh, India
ar.faridi.cs@amu.ac.in

***Abstract*— Internet of things has impacted 21st century like anything never before. Every device can be connected with each other via the internet. They can be remotely controlled or managed anytime. But all time connectivity of the IoT devices generates a huge amount of data which needs to be properly managed and disposed of as required. The data captured contains a large amount of sensitive information and patterns too; which can disclose behavioural or temporal activities. In this paper, we start by giving a brief introduction of IoT and then discuss some of its applications. After that security issues affecting IoT are discussed followed by a conclusion focusing on the need for small size & efficient cryptographic algorithms.**

Keywords—— Internet of things, IoT Layers, IoT Security & Privacy issues, IoT Applications

I. INTRODUCTION

The popularity of IoT can be determined by the study done by IHS[1] which predicts that the IoT market will increase from an initial base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025. The main aim of IoT is to connect everything which is in the household, professional, healthcare, transportation, industrial usage etc., with the internet. Due to this, these things or objects will always be available to us anywhere. IoT will greatly help in building futuristic visions [2] like robot taxi, city information model, enhanced game room etc. The huge success of IoT today was not possible without the previous researches done in the areas like wireless transmission, nanotechnology-based structures, Machine to Machine communication etc. Wireless transmission of data in the IoT devices is done either through Radio Frequency Identification (RFID) or wireless sensor network (WSN). A lot of research had already been done in the past years in these techniques and still, these areas are continuously researched.

RFID and WSN both are used simultaneously and they complement services to one another. e.g. RFID can be used to detect location while WSN can be used to sense the things present in the existing environment. Together they can enable a lot of functionalities like supply chain optimization, healthcare monitoring, inventory management etc. Since IoT uses some combination of wireless technologies, it also faces similar security issues that are present in any of these technologies and combining them will create even more security issues. The primary focus of this paper is to give a brief overview of IoT and to extensively classify the security issues in IoT and also to provide the mitigation technique along with them.

II. INTERNET OF THINGS: AN OVERVIEW

IoT in simple terms refers to connecting the devices to the internet. While wireless networks like WSN have a specific gateway node which acts as the bridge between the devices and the internet, IoT devices are usually directly connected to the internet. Since the IoT device requires unique IP addresses which is another factor to fast-track the implementation of IPv6. RFID and Sensor network is the most used wireless techniques in IoT. Initially, every IoT manufacturer wanted to create their own standard set of protocols for inter-device communication but it created compatibility issues due to the use of the heterogeneous protocols. Hence the leading manufacturers of IoT devices created a consortium. The consortium is responsible to create a specified standard set of protocols which all the member manufacturers have to agree upon. EPCglobal, Global RFID Interoperability Forum for Standards (GRIFS) are the leading standardizing protocols for RFID based communication whereas IPv6 Low-Power Wireless Personal Area Networks (6LoWPAN), ZigBee, Routing Over Low power and Lossy networks (ROLL) are major standard protocols for the sensor network.

A. Layers of IOT

Most authors generally classify IoT into three layers namely perception layer, network layer, and application layer. But some systems which provide network processing, middleware technology etc. can also be treated as an IoT layer, the middleware layer. The author in the literature [3] classifies the structure of IoT into three layers. In addition to the layers, the author also describes the threat and the requirement analysis for properly securing the IoT system. Whereas Authors in the literature [4] classify the IoT structure into five layers, the extra two layers are namely the business layer and the middleware layer. The two layers extend the IoT system by providing middleware support to the system as mentioned above and allow business logic and processing in the business layer. Authors also discuss the spintronic sensors which can be used to sense various parameters like electrical current sensing, transmission, distribution lines monitoring, vehicle detection etc. These sensors can measure the magnetic field's data out of any real-world objects, from which the required parameters related to the magnetic field can be extracted. Authors describe how IoT devices or WSN devices can be benefitted by spintronic sensors and creates new real-world applications. In another literature [5], authors also categories IoT into five layers. Other than that, they also discuss the various future applications of IoT which can be made possible in the near future. Apart from it, key challenges to IoT like naming and identity management, objects safety and

978-1-5386-6947-1/18/$31.00 ©2018 IEEE

security, spectrum crisis, green development of IoT etc. are also discussed. In this paper, we classify IoT into five layers, which are discussed in Table 1 along with their supported functions and affected layers if there is any, which are discussed in Table 1 along with their supported functions and affected layers if there is any.

TABLE I. LAYERS OF IOT

Layer	Functions of the layer	Affected things, devices or Computing
Business Layer	Business Model, graphs, flowcharts and processing of data from the application layer	
Application Layer	Smart Applications	Smart TV, Smart Car, Smart City, Smart Transportation System
Middleware Layer	IoT support systems to process or store data	Cloud computing, Expert Systems, Recommendation System
Network Layer	Data Transmission	Personal Area Network, Router, Gateways, Fog Computing
Perception Layer	Things, Objects	Sensors, actuators, RFID tag, Edge devices
Application Layer	Smart Applications	Smart TV, Smart Car, Smart City, Smart Transportation System

B. Applications of IoT

IoT has found its usefulness in various aspects. Connected devices can easily share data between them to either resolve any dependency on each other or to provide some feedback to another device upon which some work should be done. They can be completely controlled remotely too either through smart apps on the mobile devices, tablets or via a web interface. Smart cars, smart cities, smart traffic system are some of its application which was a dream for the earlier generations. IoT will allow even more applications when it will be realized fully like smart retail stores, smart power grids, smart farming etc.

1) Healthcare

a) *End-to-end connectivity* enables full diagnosis since every device is connected to each other and is sending reports constantly via Machine to Machine for patients during their treatment. The daily or real-time updates allow medical staffs to get alerts before any serious symptoms occur. It also increases affordability by saving time and money of patients by cutting down trips between hospitals, medical expenses, quality treatment etc.

b) *Patient Monitoring* has become easier due to wearable body sensors connected to IoT. Smart pacemakers, smart patient monitor, smart asthma monitor etc. have allowed medical practitioners to closely understand the patient's medical conditions. And due to this they can diagnose and treat the disease with greater accuracy.

c) *Medical diagnosis history* is the most important information about the patient. Doctors need a clear and accurate medical history to clearly understand the patient condition otherwise it may prove lethal if it is unambiguous or incorrect. IoT allows reliable transfer of these records without any destruction or loss of integrity.

d) *Data assortment and analysis* is a very important function of IoT. IoT can easily store and process a large amount of data from various healthcare devices. It also allows centralizing the patient details by collecting and integrating data from multiple sources. The data can be mined to extract useful patterns and information which can be used to predict the patient health condition.

e) *Remote medical assistance* allows the patient to get proper medical help from anywhere in the world. Often it happens that patients and their consulting doctors are separated with a significant distance. When an emergency arrives it is not always feasibly possible for consulting doctor to reach to the patient on time. But using IoT, consulting doctor can visually examine the patient remotely or can help the treating doctor to understand the patient history.

f) *Real-time reporting and monitoring* can assist patients to get their medical help or treatment before any serious symptom arises. IoT devices can not only be used to display and monitor the medical diagnostics data or parameters constantly in real time in hospitals but also in the comfort of the patient's home. If required the patient's medical condition at home can be sent remotely over a secure channel to the consulting doctor.

2) Social, Personal & home use

a) *Home automation* will be the most popular application of IoT. Imagine a person travelling to work forgot to switch off AC or lights. Using IoT, he/she can switch off them from that location away from home because the devices are connected via the internet. Or consider a person who can control its microwave oven to warm up some food before one arrives at the house. There are multiple possibilities of using IoT in homes. Anything that is used in a house can be made smart so that it can operate from its own without requiring the necessary presence of a person. It will ease up a lot of tasks, especially for elderly people.

b) *Home Security* is also a popular application of IoT. IoT can monitor any suspicious activity inside or outside the house. It can also check perimeter security of the house and warns of unauthorized access or movement in the house. It can check the health reports of various security devices and determine whether any tampering has been done or not.

c) *Energy Efficiency* will be increased in IoT. Smart bulbs, fans, AC's etc. can self-determine their optimal usage and adjust themselves to utilize power accordingly. They can also shut themselves down when not in use to save power. Devices can communicate with each other using M2M and work in tandem to optimize the house power usage. The device can self-determine when to become operational or upon receiving instructions from owners, hence increasing power efficiency.

d) *Preventing theft and loss* will be possible in IoT. IoT devices can create alerts when something is not in its place or being moved. The IoT devices can send their actual location when they are stolen to their original owners so that

they can be found instantly. Sensitive IoT device can self-destruct itself when they can't be possibly recovered.

e) *Social Networking* has become an integral part of human life. Every person wants to share their beautiful moments with their close friends and relatives. IoT eases and automates this sharing process. e.g. IoT can share the user's current location upon its request or imagine some IoT device which tracks your movement or actions and predicts what you are doing or going to do and share with your network.

f) *Smart Cities* will be the futuristic cities which can do most of its tasks automatically. Various aspects of city life e.g. road traffic management, city transportation system, power supply, smart school, smart hospitals, smart garbage collection, smart toll tax, smart meters, utility consumption fares, e-governance etc. will be easily manageable and controlled via a central hub with the help of various sensors and devices placed strategically across the city.

3) Industrial Applications, transportation, and logistics

a) *Assisted Driving* is an ongoing application of IoT. It will help drivers to safely drive their vehicles. Car owners or truck drivers will manually control their vehicle only when the automated system is unable to drive due to rough traffic or uneven road condition. Other than that owners can simply ease up and let the automated system drive the vehicle. Long road travel tires the driver and sometimes cause fatal road accidents. It will certainly help to lower these accidents.

b) *Logistics and Supply Chain* can be hugely optimized by IoT. Various sensors can monitor real-time data like the movement of goods, material movement, and other supply chain parameters and try to optimize them which in return also lowers the overall cost. It will also lower the interdependence between supply chain partners and creates reporting which can be further effectively used to develop useful production insights. Logistics will also be greatly benefited by it. Production issues, inventory management, fuel costs etc. can be monitored and predicted and thus optimizes logistics.

c) *Cargo Tracking* is another feature of IoT. Corrupt drivers, poorly loaded, overloaded cargoes are some reasons that cargoes can be lost. With the help of sensors, cargoes can be effectively fitted in the vehicle or can be continuously monitored with the help of a centralized monitoring station from the starting point to its destination.

d) *Industrial automation* can reduce the dependence on manual labour and automates various production, packaging or processing parts of industries. It can ensure a safe and coherent production flow, increase fault tolerance, decreases latency, scalable collaboration etc. [6].

e) *Industrial parametric monitoring* is another feature of IoT. IoT can deploy various sensors to collect and control various parameters like production parameters e.g. chemical concentrations, temperature, pressure etc., interoperability parameters, timing and determinism parameters, reliability and availability parameters etc. and to bring useful insights from them.

f) *Plant Safety and Security* will be ensured by IoT. IoT can provide monitoring and analytics of production parameters for production plants esp. Key Performance Indicators (KPIs) like employee leaves, vehicle accidents, property damage and other losses or damages that can occur normally in daily operations of a production plant.

g) *Quality control* is an important aspect of production. Use of good quality raw materials, the best possible produced materials, proper packaging etc. are some aspects of quality control. IoT sensor or devices can be used to identify the quality parameters of goods, pinpoint key issues and can also propose appropriate remedies for it.

TABLE II. APPLICATIONS OF IOT

Healthcare	**Social, Personal & home use**	**Industrial Applications, transportation**
End-to-end connectivity and afford ability	Home automation	Assisted Driving
Patient Monitoring	Home Security	Logistics, and Supply Chain Optimization
Medical diagnosis history	Energy Efficiency	Cargo Tracking, Industrial automation
Data assortment and analysis	Prevent theft and loss	Industrial parametric monitoring
Remote medical assistance	Social Networking	Plant Safety and Security
Real-time reporting and monitoring	Smart Cities	Quality control

C. Security Issues in IoT

IoT has created as many new problems as it had solved or maybe more. It is due to the fact that IoT devices are not secure by their nature. This insecurity is caused by the following issues. First IoT devices lie naked for the attacker as these devices generally don't change their location or even kept under constant invigilation. Hence the attacker can very easily get access to these devices and causes physically tamper to the device or destroy it completely. Secondly, IoT devices transmit their messages in an open medium which can be easily intercepted and eavesdropped by the attacker. Any insecure communication can be easily captured, modified or destroyed. The attacker might try to block the transmission by interfering with the medium. Finally, IoT devices are low powered, low processing power devices which means that it can't support complex security communication infrastructure. Simpler or old encryption technique can easily be bypassed by an attacker. Thus they become prone to attacks on their security measures. The other fact associated with this problem is that the common end user is not technologically strong to completely understand the ways and means of the security and its necessity, thus putting the responsibility of security for these devices on the device manufacturer. Any small security holes or default configurations left in the IoT device can prove very dangerous. Because first as previously discussed, the IoT devices are being used in very large numbers and they will be used in the near future too due to their inclusion in every part of human life. And second, they are being used by non-technical users who may not even know that they can be compromised. The compromised devices can be maliciously used by an attacker to further their own agenda as they did in the cases of the Mirai botnet attack in 2016 [7] and hackable Cardiac Devices from St. Jude Medical [8] etc. Thus the

manufacturer needs to be careful enough to implement and maintain the proper security measures. The manufacturer should be able to apply any security patch even using the Over The Air(OTA) technique if needed to prevent misuse of the IoT device. Researchers have identified attacks on various parts of IoT [17], [18], [19], [20]. We have classified attacks on IoT based on the layer that gets affected.

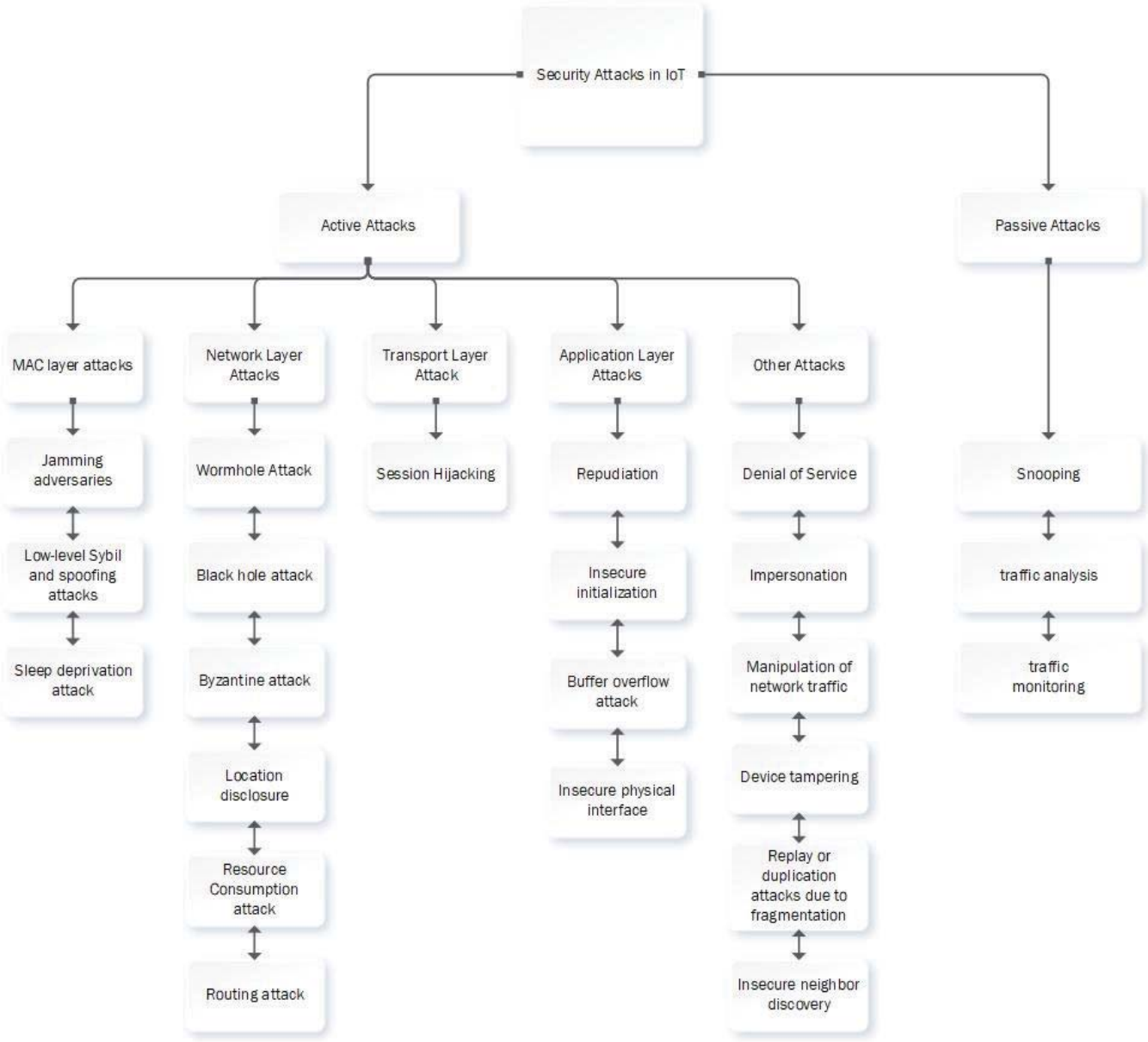

Fig 1. Security Issues in IoT

1) Active Attacks

a) MAC layer attack

Jamming adversaries [9] is a fundamental attack in IoT. Jamming is used to degrade or destroy the communications inside the network and hence affect the network performance. Jamming attacks are usually classified into two types. In reactive jamming, a rogue node will smartly determine its jamming policy to create more effective jamming attack using its sensors, whereas in conventional jamming, rogue node attacks all the nodes in the network constantly. The conventional jamming policy is energy consuming, hence inefficient. This attack can be stopped using techniques like regulated transmitted power, direct-Sequence Spread Spectrum etc.

In *Low-level Sybil and spoofing attacks*, pseudonyms or identities are faked to replace themselves with genuine nodes on the network. IoT devices use identities to distinguish themselves from other devices. An attacker can create or spoof fake but legal identity to transmit inside the network and then try to compromise or bring down the network. It can be prevented using techniques like Trusted Certification, Location Verification, Random Key Predistribution etc.

In *Sleep deprivation attack* [10], IoT devices are prevented from their regular sleep interval to exhaust their battery power. IoT devices are low powered devices, hence they go to sleep after some time intervals to save energy. This attack keeps the device awake even during its sleep

interval. It is mitigated by using an alternate source of energy like solar.

b) Network Layer Attack

In *Wormhole Attack*, at least two cooperating rogue nodes are required which shares a private link. These nodes may lie multiple hops from each other but falsely broadcasts that they have one hop distance between them. Other nodes send their data via these nodes since they foolishly believe that the advertised route is the smallest one. This can lead to another attack like sinkhole attack. It can be prevented by modifying routing protocols to secure the route selection process. Other mitigation techniques are to use trusted hardware like GPS, directed antenna etc.

In *Black hole attack* [11], [12], a compromised node is made like it has the least hop distance to every other node in the network by forging routing information during the network discovery phase. Other nodes in the network will send their data to compromised node thinking it provides the smallest path. The sole purpose of this attack is to drop all the packets it receives. They are used to collapse the network completely and can attack open loops too in the network where data flow is not congestion controlled.

In *Byzantine attack* [13], [14] security of routing protocols are attacked, two or more routers collude to disrupt the general routing services i.e. to drop, forge, modify, or misroute packets. *Location disclosure* [15] is another important aspect of IoT security. Location sensing devices extend the location services to the existing things. Though location service doesn't identify the user per se, the usage pattern i.e. constant position information along with the position of other things will eventually identify a person.

c) Transport Layer Attack

Session Hijacking is a transport layer attack. The sole purpose of *Session Hijacking* [16] is to create Denial of Service attack which is used to disrupt the network. Forged messages are created by changing TCP sequence number from valid transmissions or repeatedly creating new session establishment without using it. These techniques consume a huge amount of resources of IoT nodes due to which they can't respond to other valid nodes, thus creating a Denial of Service attack.

d) Application Layer Attack

Repudiation attack is done to deny any or all participants in the communication of information. This attack can lead to loss of information or transmission of false information. IoT devices are needed to be carefully initialized and configured which ensures proper functioning of the entire network to prevent any privacy leakage or network disruption. But In *Insecure initialization*, the network is not allowed to do so. Communication needs to be protected at lower levels too.

Buffer overflow attack [16] is a common application layer attack. In this, application buffers are overflowed such that protected memory space can be attacked to inject malicious code or corrupt the current application state. *The insecure physical interface* can create a huge problem. An attacker can easily acquire privileged access to the firmware which can lead to leakage of any type of information or disrupt the network by network or transport layer attacks.

e) Other Attacks

Denial of Service is the stopping of normal operations or services provided by the IoT devices. DoS can be created by rogue nodes in the network or attacks on the application layer. *Impersonation* [21] is used by hackers for mimicking a physical node or a group of virtual nodes. It may not be as harmful to devices based on wireless sensor network as to RFID based devices. Physical layer imperfections in individual RFID devices make them prone to this attack.

Manipulation of network traffic is done to capture sensitive information of users. IoT devices capture various information during its operation. This information can be used to extract sensitive information like sleeping patterns, commute intervals, behavioural profiling etc. In *Device tampering*, attackers tamper the firmware of the IoT device to insert their malicious code. The code runs silently in the device and capture and transmitting sensitive information to its attacker.

Replay or duplication attacks due to fragmentation [22] happens because of the difference between IPv6 packet length and 6LoWPAN packet length. IPv6 packet length is much bigger than the 6LoWPAN packet length and the IPv6 packet needs to fit in the 6LoWPAN packet thus requiring fragmentation. But fragmentation services should be done only at the sender and receiver side in the adaptation layer but the security mechanisms are not defined yet. An attacker can create its own custom packet with different fragmentation field such as datagram size, datagram offset etc. which can cause a buffer overflow, rebooting, resource exhaustion etc.

Insecure neighbour discovery is a very serious security concern. Nodes need to find a path between sender and receiver along with router discovery and name resolution before it can transmit messages. Therefore it sends neighbour discovery packets to get the network topology. But insecure neighbour discovery packets without proper verification can prove harmful for network and may lead to denial of service.

2) Passive Attacks

a) Snooping or eavesdropping is the most common form of passive attack. An attacker passively listens to all communication going inside the network and extracts sensitive information from it. Unsecured transmission is easier to snoop and secured transmission.

b) *Traffic analysis* is similar to snooping except instead of extracting sensitive information directly, it looks for useful patterns from which it can extract information.

c) *Traffic monitoring* is similar to other passive attacks. It constantly monitors traffic and records similarities and pattern.

III. Conclusion & Future works

In this paper, we have started with a brief overview of IoT. Then we discuss the major security issues in IoT. The security issues are classified according to the networking layers that get affected by them. IoT is an exciting field. It has a lot of areas that are still left to explore. The reach of IoT in human society has not been fully determined yet. It has breakthrough potential like the Internet which connected billions of people around the world [23]. So it is much imperative for people related to IoT esp. security researchers to thoroughly understand the security concerns and to make strong mitigation strategies to prevent its abuse. Security

holes in IoT can pose a serious danger because billions of IoT devices will be used to automate a large number of processes in every household. Their proximity to human society and the grunt work they do which allows users to focus on more important tasks, affects millions of people simultaneously. The conventional security practice is not suitable for IoT as they require comprehensive security checks and complex algorithms which are power hungry and computationally expensive. Whereas IoT devices are low power, low computation devices. Security algorithms for IoT must be energy efficient, low-weight and which requires fewer CPU cycles to implement the security system. Elliptic curve cryptography [24], [25], [26] applications are suitable for IoT but newer security algorithm like Code-based cryptography [27] can also be explored to achieve greater security. The future work will be to create a survey paper which focusses on the recent developments in IoT and the remaining issues that require the researcher's focus. The survey paper will extensively aggregate the security issues of IoT, a detailed taxonomy, security policies and mitigation strategies.

REFERENCES

[1] Columbus, L. (2016, November 27). Roundup OfInternet Of Things Forecasts And Market Estimates, 2016. Retrieved October 17, 2018, fromhttps://www.forbes.com/sites/louiscolumbus/2016/11/27/roundupof-internet-of-things-forecasts-and-market-estimates-2016/

[2] Datta, P., & Sharma, B. (2017, July). A survey on IoT architectures,protocols, security and smart city based applications. In Computing, Communication and Networking Technologies (ICCCNT), 20178th International Conference on (pp. 1-5). IEEE.

[3] Zhuankun Wu. : Initial Study on IOT Security architecture. J.Strategy and decision-making research (2010)

[4] Liu, X., Lam, K. H., Zhu, K., Zheng, C., Li, X., Du, Y., ... & Pong, P.W. (2016). Overview of Spintronic Sensors, Internet of Things, andSmart Living. arXiv preprint arXiv:1611.00317.

[5] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December).Future internet: the internet of things architecture, possible applications and key challenges. In Frontiers of Information Technology(FIT), 2012 10th International Conference on (pp. 257-260). IEEE.

[6] Breivold, H. P., & SandstrÃ˝um, K. (2015, December). Internet ofThings for Industrial Automation–Challenges and Technical Solutions. In Data Science and Data Intensive Systems (DSDIS), 2015IEEE International Conference on (pp. 532-539). IEEE.

[7] Woolf, N. (2016, October 26). DDoS attack that disrupted internet was largest of its kind in history,experts say. Retrieved October 26, 2018, fromhttps://www.theguardian.com/technology/2016/oct/26/ddosattack-dyn-mirai-botnet

[8] The FDA confirmed that St. Jude Medical's implantable cardiacdevices have vulnerabilities that could allow a hacker to accessa device. Once in. (2017, January 09). FDA confirms that St.Jude's cardiac devices can be hacked. Retrieved October 26,2018, from https://money.cnn.com/2017/01/09/technology/fda-stjude-cardiac-hack/

[9] Tang, X., Ren, P., & Han, Z. (2018). Jamming Mitigation via Hierarchical Security Game for IoT Communications. IEEE Access, 6,5766-5779.

[10] I. Andrea, C. Chrysostomou, and G. Hadjichristofi. Internet ofthings: Security vulnerabilities and challenges. In Proc. of 2015 IEEESymposium on Computers and Communication (ISCC), July 2015.

[11] Ali, S., Khan, M. A., Ahmad, J., Malik, A. W., & ur Rehman, A.(2018, April). Detection and prevention of Black Hole Attacks inIOT & WSN. In Fog and Mobile Edge Computing (FMEC), 2018Third International Conference on (pp. 217-226). IEEE.

[12] Roy, S. D., Singh, S. A., Choudhury, S., & Debnath, N. C. (2008, July).Countering sinkhole and black hole attacks on sensor networksusing dynamic trust management. In Computers and Communications, 2008. ISCC 2008. IEEE Symposium on (pp. 537-542). IEEE.

[13] Yu, M., Zhou, M., & Su, W. (2009). A secure routing protocol againstbyzantine attacks for MANETs in adversarial environments. IEEEtransactions on vehicular technology, 58(1), 449-460.

[14] Fragkiadakis, A. G., Tragos, E. Z., & Askoxylakis, I. G. (2013). Asurvey on security threats and detection techniques in cognitiveradio networks. IEEE Communications Surveys & Tutorials, 15(1),428-445.

[15] Elkhodr, M., Shahrestani, S., & Cheung, H. (2014, June). A semanticobfuscation technique for the Internet of Things. In Communications Workshops (ICC), 2014 IEEE International Conference on (pp.448-453). IEEE.

[16] Teixeira, F. A., Machado, G. V., Fonseca, P. M., Pereira, F. M., Wong,H. C., Nogueira, J. M., & Oliveira, L. B. (2014, May). DefendingCode from the Internet of Things against Buffer Overflow. InComputer Networks and Distributed Systems (SBRC), 2014 BrazilianSymposium on (pp. 293-301). IEEE.

[17] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchainsolutions, and open challenges. Future Generation Computer Systems, 82, 395-411.

[18] Lupu, T. G., Rudas, I., Demiralp, M., & Mastorakis, N. (2009,September). Main types of attacks in wireless sensor networks. InWSEAS international conference. proceedings. recent advances incomputer engineering (No. 9). WSEAS.

[19] El Mouaatamid, O., Lahmer, M., & Belkasmi, M. (2016). Internetof Things Security: Layered classification of attacks and possibleCountermeasures. Electronic Journal of Information Technology,(9).

[20] Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. arXiv preprintarXiv:1707.01879.

[21] ÄNolakoviÄ ˇ G, A., & HadÅ¿ialiÄ ˇ G, M. (2018). Internet of Things (IoT): ˇA Review of Enabling Technologies, Challenges, and Open ResearchIssues. Computer Networks.

[22] Kim, H. (2008, August). Protection against packet fragmentationattacks at 6lowpan adaptation layer. In Convergence and HybridInformation Technology, 2008. ICHIT'08. International Conferenceon (pp. 796-801). IEEE.

[23] "World Internet Users Statistics and 2018 World Population Stats."World Internet Users Statistics and 2018 World Population Stats,www.internetworldstats.com/stats.htm.

[24] Marin, L., Pawlowski, M. P., & Jara, A. (2015). Optimized ECCimplementation for secure communication between heterogeneousIoT devices. Sensors, 15(9), 21478-21499.

[25] Win, E. K., Yoshihisa, T., Ishi, Y., Kawakami, T., Teranishi, Y., &Shimojo, S. (2018). Lightweight and Secure Certificateless Multireceiver Encryption based on ECC. Journal of Information Processing, 26, 612-624.

[26] Sarwar, K., Yongchareon, S., & Yu, J. (2018, August). Lightweight ECCwith Fragile Zero-Watermarking for Internet of Things Security. In2018 17th IEEE International Conference On Trust, Security AndPrivacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 867-872). IEEE.

[27] Sendrier, N. (2017). Code-based cryptography: State of the art andperspectives. IEEE Security & Privacy, 15(4), 44-50.