Internet of Things in Smart City Environments

Sanjay Kumar Gupta, S.B. Vanjale

Abstract*: With the advent of smart devices, a huge paradigm shift is observed in the way the users define service quality. Further, these devices or Internet of Things (IoT) devices as they are generally addressed, have acted as catalyst for comfort and connectivity and are building blocks of Smart City environment. With limited thought related to security is involved during the deployment of such devices, they offer a dangerous environment of opportunity to the attackers from the internet; which not only jeopardize network security, bus also the privacy of the users. Hence, it is of utmost importance to address the security concerns in smart city environment. This paper attempts to study the current IoT technologies deployed in a smart-city environment along with its vulnerabilities and possible solutions to improve IoT security. An approach is made to study the various vulnerabilities available with the IoT devices deployed in the smart city setup, various motivation of an attacker and the analyse some of the recent attacks witnessed by IoT devices. A few possible solutions for mitigation are suggested in this paper. The findings of the paper can be implemented in any network of IoT devices.

Keywords: IoT, IoT security, Smart city, Vulnerability.

I. INTRODUCTION

In the last decade, with the rapid development of access technologies, there has been exponential growth of on-demand services available to the end -users [1].With the ease of connectivity, availability of high processing power and large scale information sharing, users are expecting to control their desired environment like home, work-space etc. irrespective of their physical location and distance This has led to the birth of smart devices which are rudimentary devices having embedded technology to communicate and interact with external environment[2]. With millions of such devices being deployed every day, a platform to interconnect the network of several objects and devices is defined as “Internet of Things” (IoT) [3].Presently crucial applications like home security, traffic management, resource management etc are fast becoming a interconnection of millions of embedded devices [4] Its is estimated that by 2020 IoT environment will comprise of 26 billion devices[5].

The deployment of IoT in smart environment stems from objectives of a typical smart city required for e-governance. These may include[6]:a) Optimization of Public services like traffic flow, parking, garbage management, city-lighting, surveillance of hospitals, schools and other public areas, b) Optimization of resources like water supply management, electricity management, allocation of civic staff etc; c) Traffic Management for reduction in congestion , d) Monitoring of City Environment viz. Air Quality index monitoring, pollution monitoring etc; e) Better and Transparent Government viz. providing on-demand services to the citizens and f) Reducing Operational Costs by smart usage of energy and automation of mundane tasks.

The IoT devices generally connect to the network by wireless access technologies [6]. With the growth of 4G and 5G access technologies across the globe more and more applications are being added for seamless control of the user environment for further augmenting the user experience of service [7] thereby empowering IoT deployments. With rapid research being undertaken across the globe for IoT devices, Smart parking, Smart Traffic controls and smart watches are acting as pioneers in smart city environments [6].

Due to mass production of IoT devices, limited security measures are incorporated by manufacturers [8] to limit the cost of deployment. These has resulted in alarming rise in hacks and breaches in the IoT setup deployed, which are of dangerous consequences[9]. In 2018 security bulletins [10] published by various security agencies and manufacturers, IoT security is always marked as top concerns. By considering the role of such devices in the day-to-day life of end users and the fact that compromise of devices by attackers can cause unprecedented damage in the environment of focus of the users, security needs to be implemented as a core feature of such devices [10].

The paper is organized in five sections. Section-I reviews the concept of IoT and its purpose in smart city environment. Section -II analyses the basic components of IoT. A study of vulnerabilities and their exploits are carried out in Section -III. Possible solutions and future steps are presented in Section-IV and finally conclusions are drawn in Section –V

II. INTERNET OF THINGS (IOT)

Internet of Things (IoT) is a network of items embedded with sensors, software and network connectivity that collect and exchange information [11]. Over the past few years, domains of production engineering, medical electronics, automation, electrical and intelligent computational systems are integrated into IoT[12]. With rapid deployment of IoT across all the engineering domains, for seamless interconnection of the devices and to use the existing internet architecture for device deployment, standardization of protocols and IoT stacks are desired.

Manuscript published on 30 September 2019
* Correspondence Author

Sanjay Kumar Gupta*, Faculty of Interdisciplinary Studies (Computer Engineering), Bharati Vidyapeeth (Deemed to be University), Pune, India. Email: skgru@yahoo.com

S.B. Vanjale, Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University), Pune, India. Email: sbvanjale@bvucoep.edu.in

*Retrieval Number: C6618098319/19©BEIESP
DOI:10.35940/ijrte.C6618.098319*

The standardization is designed keeping in mind the IoT device characteristics which include [13] low energy sensor devices, low processing power and low bandwidth of operation. These standards as defined by Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE) enables the devices to communicate with external entities in the internet[14]. The standardization effort in IoT has contributed to the concept of IoT protocol stack which is presented in Fig. 1[13].

Considering the limited processing power of the IoT devices, UDP protocol is presented in the transport layer as it provides smaller overhead as compared to TCP protocol [13].

IEEE802.15.4[15] provides the standardized equivalence of OSI model’s Physical and Datalink layers for Low Rate Wireless Personal Area Networks (LRWPANs)[16]. The MAC layer which is also called Data Link layer, is the means for communication between two devices based on contention mechanism. It implements Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme together with a deterministic mechanism. The Physical layer transmits the MAC frame through the medium supporting various frequency bands.

RFC4944[17] defines the IPv6 Over Low Power Wireless Personal Area Network (6LowPAN). It basically compresses IPv4 packets in IEEE802.15.4 frames. It paves the way for interconnecting IoT devices on the existing IP network infrastructure.

RFC7252[18] defines Constrained Application Protocol (CoAP), which is a message exchange application layer protocol for low energy low power bandwidth limited network, hence is suitable for IoT operations. This protocol is widely used in machine-to-machine applications, a paradigm used in IoT automation [18].CoAP doesn’t include security features[13], however it supports TLS for UDP protocol[19]

III. VULNERABILITIES AND THEIR EXPOLITS IN IOT

6LoWPAN and CoAP protocols reduce the difference between internet and IoT protocols, but due to constraints laid down by IoT, there is a huge difference in their specifications. These differences act as a major obstacle for implementing security between IoT and Internet devices [20]. Security requirements of an IOT device must include the dataflow of communication among sensor devices [13].

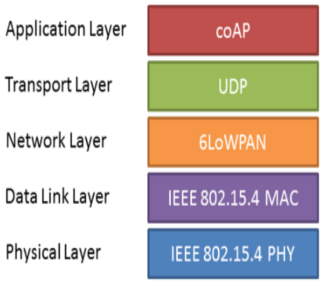

Fig. 1. IoT Protocol stack[13].

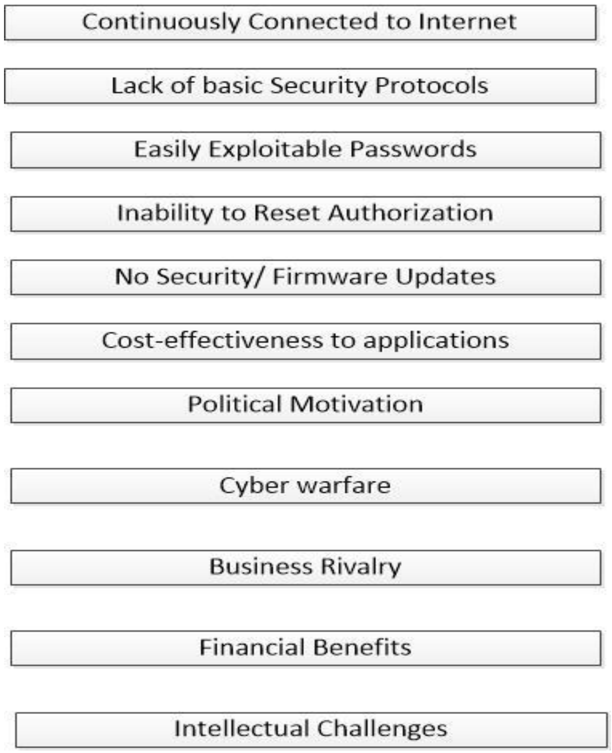
Continuously Connected to Internet
Lack of basic Security Protocols
Easily Exploitable Passwords
Inability to Reset Authorization
No Security/ Firmware Updates
Cost-effectiveness to applications
Political Motivation
Cyber warfare
Business Rivalry
Financial Benefits
Intellectual Challenges

Fig. 2. Motivation of attacks on IoT Devices [6]

While IoT has many potential benefits across domains, from security perspective, it also provides a lucrative motivation to the attackers [6]. These motivations are graphically presented in Fig.2 [6].It may be assumed that an attacker may consider these motivations as an opportunity to exploit the same for malicious intent [6]. The goals of the attackers may include [13]: DDoS attack on internet, breach of privacy, extortion from the users, forging of critical data, illegal data mining, or coordinated attack like cyber warfare. For a Smart-city environment, the IoT devices under threat of attacks include [6]various digital sensors, security cameras, digital-locks, smart wearable devices, hubs, personal electronic devices, usernames and passwords, biometrics stored in devices etc. In order to secure such devices their attributes viz. Confidentiality, Integrity, Availability, Authentication, Authorization and Non-repudiations are of key importance[6]. Any system module which lacks any of these attributes may be considered vulnerable and at risk. For example a smart CCTV-camera manufacturer develops the device firmware, hardware interfaces, software app and cloud platform. A breach in any one of the components or in the connectivity between the components poses a threat to all.

IoT devices have web interfaces which connect to the information servers. SQL injection and cross-website scripting may impact the web interfaces [21].In SQL injection , the attacker enters a malicious SQL code in field which is accessed by the application’s SQL engine and can result in privilege escalations and other access issues for the devices.

In Cross website scripting a malicious code is executed in the system by the attacker and is sent to a target by the compromised interface giving rise to DoS attack. Other vulnerabilities may include [13] weak authentication, unencrypted communication between devices, credentials stored in plain text, lack of file system encryption, lack of verification of software updates, no isolation zone defined in network.

These had resulted in threats like [13] interception of communication, man in the middle attack, data compromise, forced authentication, credential stealing firmware corruption etc.

Recently discovered Wifi vulnerability KRACK[22] add to the security concerns of IoT as they majorly depend on Wifi for interconnectivity. Similarly Sybil Attacks[23]causes routing confusions in wireless domain which may severely impact geographic routing procedures, data aggregation and resource allocation and drain the system resources.

Most attackers take advantage of the default credentials used by vendors which are left unattended by the users. The most dreaded DDOS attack involving IoT is conducted by Mirai botnet[24] originates from this fact. It scans the target IoT device for open ports , once available it uses known combinations of default credentials to brute-force authentication. Once compromised, the malware turns the device as botnet to launch automated DDoS attacks.

Similarly software updates are generally not followed in regimen by the device manufacturers as well as end-users thereby increasing the risk of exploitation of the vulnerabilities by the attackers [25]. Based on the discussions presented in the previous sections the possible attacks exploiting the various layers of the IoT protocol stack is summarized in Fig.3.

Latest malicious activities involving IoT [11] includes Device cloning and un authorized control of IoT devices. In device cloning a foreign hardware can spoof itself as a authentic device and can scale up in a IoT environment like smart cities. The malicious data thus generated by such attack can cause overload of important server resources, costing massive time and budget to fix the issue. Unauthorized control of IoT devices may lead to breach in user privacy, security and even jeopardizing the life of citizens if critical areas are like hospital management, emergency services etc are compromised. The recent DDoS attacks employing IoT devices are presented in Table-I.

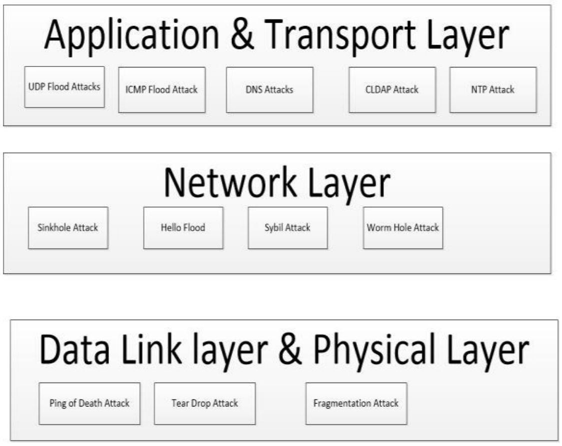

Fig. 3. DDoS Attacks on various layers of Protocol Stack[21][22][23]

Table -I: List of the recent DDoS attacks employing IoT Devices [24].

Sr. No	Name of Attack	Year of attack	Target	Activity
1	BashLite	2015	Cameras, DVRs	The attacker by passes the security protocols by Brute-force on telenet. It causes UDP/TCP flooding and HTTP attacks with a Volume capacity of 400 Gbps
2	Mirai	2016	CCTV camers, DVR and Routers	It results in large volume of 1.1 Tbps DDoS attack using 150,000+ IoT devices. It uses default credentials of connected devices. It can infect 4000 Iot devices every hour. It causes attacks such as SYN and ACK, UDP Flooding, HTTP traffic, DNS attacks
3	Reaper	2017-18	All IoT devices including CCTV cameras, Routers	It exploits security vulnerabilities present in the code of IoT devices. It implements a light programming language LUA to launch DDoS attacks on Iot devices

IV. POSSIBLE SOLUTIONS AND FUTURE STEPS

As can be seen in our immediate surroundings, IoT devices have become an integral part our life. Hence securing the IoT devices are of paramount importance. Personal data like the camera feeds, biometrics etc. captured by IoT Devices in a smart city environment if not handled properly poses a risk to user’s privacy. The first step towards implementing the security involves implementation of strong authentication mechanism to prevent hijacking and botnet proliferation.

Retrieval Number: C6618098319/19©BEIESP
DOI:10.35940/ijrte.C6618.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The same can be performed by including the following in the Security management system of the IoT setup [25]

- Ensure the default passwords are changed to strong passwords and are updated in a well-defined time bound manner
- Update the security patches of IOT devices as and when available
- Disable universal plug and play without proper device authentication and administrative permission
- Inspect the network services available and connected to the environment
- Inspect the communication between devices
- Wherever possible encrypt the communication between the devices and network
- Implement filter based firewalling in the networking devices to filter out malicious requests.
- Educate the end users about the security and privacy concerns.

Current IoT deployments use data protocols that offload security to TLS. This poses a greave problem as device manufacturers constraint with economies of scale neglect configuring separate TLS for their devices and prefer to use the default available, posing a grave threat to the setup. A possible solution is to develop a new data protocol based on CoAP with security feature which is easy to use and is reliable. The solution needs to be easier than TLS configuration, while offering confidentiality, integrity, authentication and other security features.

For implementing future-proof and long term solutions for IoT security, it is recommended to build defence against the deadly robotic-botnets in the IoT environment. Defences against Botnets which causes the DDOS attacks can be implemented by the following steps:

- Preventing botnet infections
- Monitoring the activities
- Response to attack for neutralizing the botnets.

Prevention can be carried out by implementing antivirus software , complemented by IDS/IPS setup ,content filtering firewall and whitelisting. This should be supplemented by user awareness methods like not opening un-solicited email attachments etc. Regular monitoring of the network resources and assets should be carried out to detect device behaviour for anomalous trends that might indicate presence of threats. Network monitoring tools should be installed in the setup to flag departures from established baseline for traffic volumes, bandwidth use, protocol use and other metrics. On the event of detection of a botnet quick response like disconnection, neutralizing botnet etc may be implemented to ensure secure environment for IoT deployments.

Hence for a holistic approach of security concerning the security and privacy on a IoT deployment, as explained in Fig. 4, following suggestions may be implemented as a part of the security policy [25]

V. CONCLUSIONS

IoT is changing the way the end users view the services offered by the service providers. Governments across the globe are implementing smart cities for providing citizens a platform for e-governance. Even though much standardization has been defined by various standardization bodies for seamless interconnection of these devices with the existing internet technologies; due to the economies of scale and reach of the IoT devices very limited concentration is provided by end-users, service providers and manufacturers towards security implementation in such devices. This had let to various attacks on the networks which has devastating effects for end users. This paper reviews the basic concepts of the IoT including its standardized architecture. Later a study is made on the various vulnerabilities observed in the IOT and how the attacker exploits the same with little efforts. As a future perspective to secure the smart city environment and to protect the IOT infrastructure from being misused and jeopardizing personal security of the end-users, discussion is made on the various steps to be implemented for a secure experience in the network. As e-governance is for spread of democracy, similarly in order to secure the smart city environment from possible cyber attacks, manufacturers, developers, network providers and end users need to join hand to empower the network against possible cyber-attacks

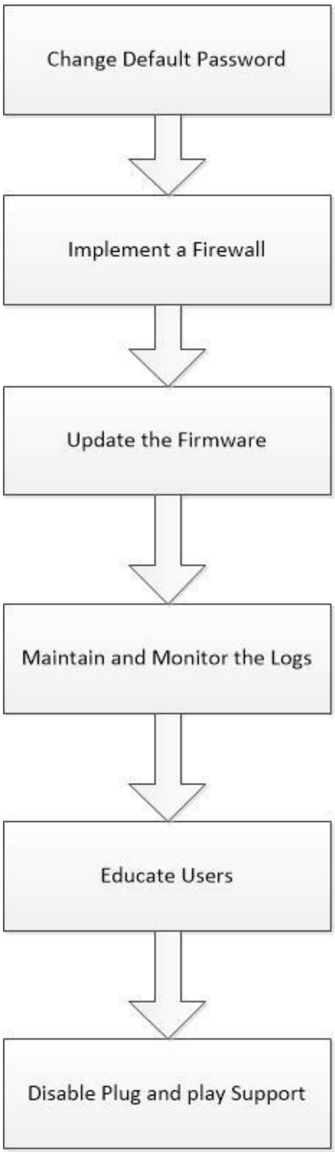

Fig. 4. Suggestion for Security Policy [25]

REFERENCES

1. M. Ray , M.Chandra, B.P.Patil, "Scalable Hybrid Speech Codec for Voice over Internet Protocol", *International Journal of Advanced Computer Science and Applications,*Vol. 7,Issue 4,190-197,2016
2. Gartner IT Glossary- Internet of Things definition.Available online at *https://www.gartner.com/it-glossary/internet-of-things* Accessed in January 2019.
3. S.Mishra, P.V. Krishna, H.Agarwal, A.saxena,M.S.Obaidat, "A Learning automata based solution for preventing DDoS in IoT.", *IEEE 4th International Conference on Cyber, Physicaland Social Computing",* 144-122, 2011.
4. A.R.Sadeghil, C.Wachsmann, M.Wainder, "Security and Privacy challenges in Industrial IoT",*ACM Proceedings of 52nd Annual Design Automation Conference,* 7-11, 2015
5. Gartner Press Release. Available online at *https://www.gartner.com/newsroom/id/3598917* Accessed in January 2019
6. D.Bastos, M.Shackleton, F.E.Moussa, "IoT: A survey of Technologies and Security Risks in Smart Home and City Enviornment", *Proceedings of IET Conference on Living in the Internet of Things: Cybersecurity of the IoT,* 1-7 *, 2018.*
7. M.Ray, M.Chandra, "Evaluation of Wavelet-based speech coders for VoIP Applications", *Proceedings of the International Conference on Nano-elctronics, circuits & Communication Systems. Lecture notres in Electrical Engineering",*vol. 403, 29-37, 2017
8. M.E.Ahmed, H.Kim, "DDoS Attack Mitigation in IoT Using SDN", *IEEE 3rd International Conference on Big data computing services and applications,* 271-276, 2018
9. IOT Security Foundation Guidelines. Available online at *https://www.iotsecurityfoundation.org/best-practice-guidelines/* Accessed in January 2019
10. Trend Micro Security Predictions for 2018. Available online at https://resources.trendmicro.com/rs/945-CXD-062/images/rpt-paradigm-shifts.pdf? Accessed in February 2019.
11. S. Naik, V.Maral, " Cyber Security – IoT", *2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology,* 764-767, 2017
12. Y.Seralathan ,T.Oh, S.Jadhav, J.Myers, J.Jeong, Y.H.Kim, J.N.Kim, "IoT Security Vulnerability:A Case Studyof a web Camera", *IEEE International Conference on Advanced Communications Technology ,* 172-177, 2018
13. L.A.B Pachero, J.J.C Gondim, P.A.S.Barreto, E.Alchieri, " Evaluation of DDoS threat in IoT", *IEEE 15th International Symposium on Network Computing and Applications,* 89-92, 2016
14. J.Granjal, E.Moneterio, J.S.Silva, "Security for the IoT: A Survey of existing Protocols & open research Issues",*IEEE Communications Surveys & Tutorials,* Vol.17, no.3, 1294-1312, 2015.
15. IEEE, *Wireless Media Access Control(MAC) and Physical Layer (PHY) Specifications for Low rate Wireless Personal Area Networks(WPANs),* IEEE Styandard for Information Technology, 2011.
16. Information Technology- Open Systems Interconnection- Basic Reference Model: The basic model , 1994
17. G. Montenegro,N.Kushalnagar, J.Hui, " RFC 4944 : Transmission of IPV6 packets over IEEE802.15.4, 2007.
18. Z.Shelby, K.Hartke, C.Bormann,, " RFC 7252: The Constrained Application Protocol", 2014
19. E.Rescorla, N.Modadugu, "RFC 4347: DTLS- Datagram Transport layer Security", 2006
20. J.Hui, P.Thubert, " RFC 6282: Compression format for IPV6 datagrams over IEEE 802.15.4-based networks", 2011
21. B.Dorsemaine, " A New approach to investigate IoT threatsbased on 4 layer model", *IEEE 13th International Conference on New Technologies for Distributed Systems, ,* 2016
22. Key Reinstallation Attacks causes and actions Available online *https://www.krackattacks.com* Accessed on April 2019
23. J.R. Douceur, " The Sybil Attack", *Springer 1st International Workshop on Peer-topeer systems,* 251-260, 2002
24. H.Sinanvoic, S.Mrdovic, "Analysis of Mirai Malicious Software", *25th IEEE International Conference on Software, Telecommunications and Computer Networks,* 1-5, 2017
25. J.Singh, T.Pasquier, J.Bacon, H.Ko, D.Eyers, " 20 Security Considerations for the cloud supported IoT", *IEEE IoT Journal* Vol.3 Issue 3, 2016

AUTHORS PROFILE

Sanjay Kumar Gupta received his Master's Degree in Physics with Specialization in Electronics from Garhwal University, Srinagar, Uttarakhand. He has obtained ALCCS degree in Computer Science from IETE, New Delhi. He has over 26 Years of Experience in Software development, test and evaluation of application software, formulation and Implementation of various Information & Communication Technology applications across Domains and extensive experience in IT, ITeS and ESDM sectors. He is Pursuing PhD from Bharati Vidyapeeth (Deemed to be University), Pune, Maharashtra. His area of interest includes IP Networking, Peering Technologies, Internet technologies, AI, IoT, High Speed Data communication networking. Wireless and terrestrial networks and network security

S.B. Vanjale, received B.E. Computer Engineering from Shivaji University, Kolhapur , Maharashtra, M.E and PhD. in Computer Engineering from Bharati Vidyapeeth (Deemed to be University), Pune, Maharashtra. He is working as Professor in Computer Engineering Department of Bharati Vidyapeeth (Deemed to be University), Pune, Maharashtra. He has got more than 19 Years of teaching experience and guided more than 200 BE students, 25 Post Graduate students and 1 PhD student in the field of Computer Engineering. He has published more than 80 research papers in the area of Information Technology in reputed International Journals. His areas of interest include Internet Technologies, IoT and Advanced computing, Wireless Networks, Network Security.

Retrieval Number: C6618098319/19©BEIESP
DOI:10.35940/ijrte.C6618.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication