INTERNET OF THINGS: TAXONOMY OF VARIOUS ATTACKS

Abhishek Raghuvanshi[1]
Department of Computer Science & Engineering
Mahakal Institute of Technology
Ujjain, India

Dr. Umesh Kumar Singh[2]
Director
Institute of Computer Science, Vikram University
Ujjain, India

Prashant Panse[3]

Associate Professor, Department of IT, Medi-Caps University, Indore

Monika Saxena[4]

Banasthali Vidyapith, Jaipur, Rajasthan 304022

Ravi Kishore Veluri[5]

Associate Professor, Aditya Engineering College

Abstract:

IoT is a combination of conventional systems, sensors, clouds, smartphone apps, online applications and control systems that influence every part of people's lives. With increasingly heterogeneous devices and data processing, security issues are growing. The fact that most IoT software and systems are not entirely protected and vulnerable to such threats is often widely understood. On average, 60% of IoT software and gadgets are correlated with some type of vulnerability. It is becoming easier for an adversary to hack into a program, make it unusable, or capture sensitive information and data. The impact of the different threats varies considerably: some affect the security or quality of the records, while others affect the availability of the device. At present, companies are trying to recognize what the risks to their information assets are and how to access the appropriate means to tackle them, which appears to be an obstacle. To improve understanding of security threats, this paper summarizes IoT

security attacks and establishes taxonomy based on the application domain and the design of the architecture.

Keywords:* *IoT security, Vulnerability, Threats, Attacks, Three Layer Architecture, Taxonomy

1. Introduction

IoT converts objects from old to smart by applying its basic developments, for example, in viewing computation, correspondence, Internet norms, and applications. Consolidation of sensors, hardware and connectors has made it smarter and more accessible to us, leading to a happier human life, more housing, better welfare, protection and better use of features. Protection requirements for IoT are also growing due to the rapid growth of heterogeneous devices and applications. [1]

The threat, the vulnerabilities, and the attack must be defined in order to understand IoT security. Any future vindictive incident which may hurt an advantage is a hazard. Vulnerability is a weakness that renders a hazard imaginable. This may be attributed to faulty plans, configuration botches, or inadequate and unclear coding procedures.

An assault is an action that exploits or authorizes a threat from vulnerability. Instances of attacks include the submission of a vindictive contribution to an application or the flooding of a device seeking to deny assistance.

The CloudFlare services help Wikipedia defend itself from attacks. This approach is effective because CloudFlare has considerable expertise in the handling of such attacks. This is a truly exciting time for online encyclopedias. For eg, Spamhous was protected in March 2013 by CloudFlare's services. Furthermore, CloudFlare Client GitHub (an online coding site)[2] was targeted in August 2015 by a DDoS attack by hijacking unsatisfactory web browsers.

Figure 1 shows that 63 percent web applications suffers from cross site scripting and 51 percent web applications suffers from information leakage.

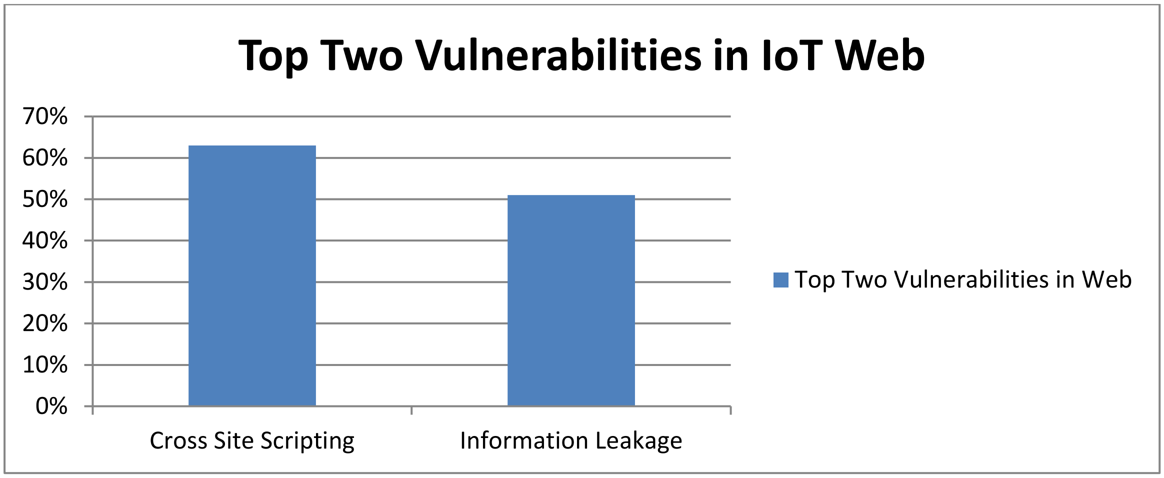

Fig.1. Vulnerabilities in IoT Web Applications

On 28 February 2018, the most damaging one was published. This threat has been mitigated by Akamai's Prolexic DDoS operation. Akamai has invested in security with high-DDoS. It consists of seven scrubbing centres and 150 staff working to counter DDoS attacks. It is also obvious that it takes immense amounts of capital, energy and time to spend. While such attacks remain vulnerable to a significant number (approx. 50 K) of memcached servers[3].
The DDoS assault on Botnets in October 2016 compromised a large number of IoT-based devices[4]. Few standard DDoS attacks endanger the networks of rail transport. In October 2017, the DDoS attacks struck the rail network in Sweden, delaying the operation, collapsing the IT infrastructure that tracks the location of the trains, and dismantling the related email networks, websites and traffic maps. IoT protection is also the hour needed to deliver stable and seamless services in an IoT environment for today's network media.

Section 2 contains three layer architecture of internet of things. Section 3 contains taxonomy of various security attacks in internet of things. Section 4 contains conclusion and future challenges.

2. Internet of Things Architecture:

The three-layer architecture consists of application layer, network layer and perception layer [5][6][7]. It is shown below in figure 2.

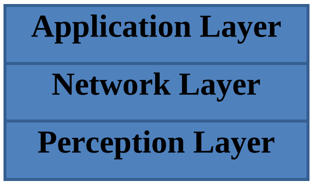

Fig.2. Three Layer Architecture

- **The Perception Layer**

The first layer is the vision layer. Basically, this layer handles the objects that are known, collecting data from the things. It includes RFID labels, QR code, and numerous types of sensors that coordinate 2-D scanner tag marks and readers by camera, terminals, and remote sensor. The principal skill of this layer is to greatly identify the objects and collect the data.

- **The Network Layer**

The network layer is often referred to as the layer for transmission. This layer collects the information from the layer of perception and transmits the information to the IOT devices safely. This layer manages several devices such as firewall, hub and switch for networking.

- **The Application Layer**

The framework layer resides between the market layer and the middleware layer. The platform layer provides consumers with application-related resources. In this sheet, there could be several apps, including: smart health, smart house, smart environment, smart vehicle, smart farming, smart logistics, smart transport, etc.

3. **Taxonomy of Attacks in Internet of Things:**

Figure 3 presents taxonomy of attacks in internet of things. This taxonomy is prepared on the basis of three layer architecture. It contains attacks at perception layer, network layer and application layer.

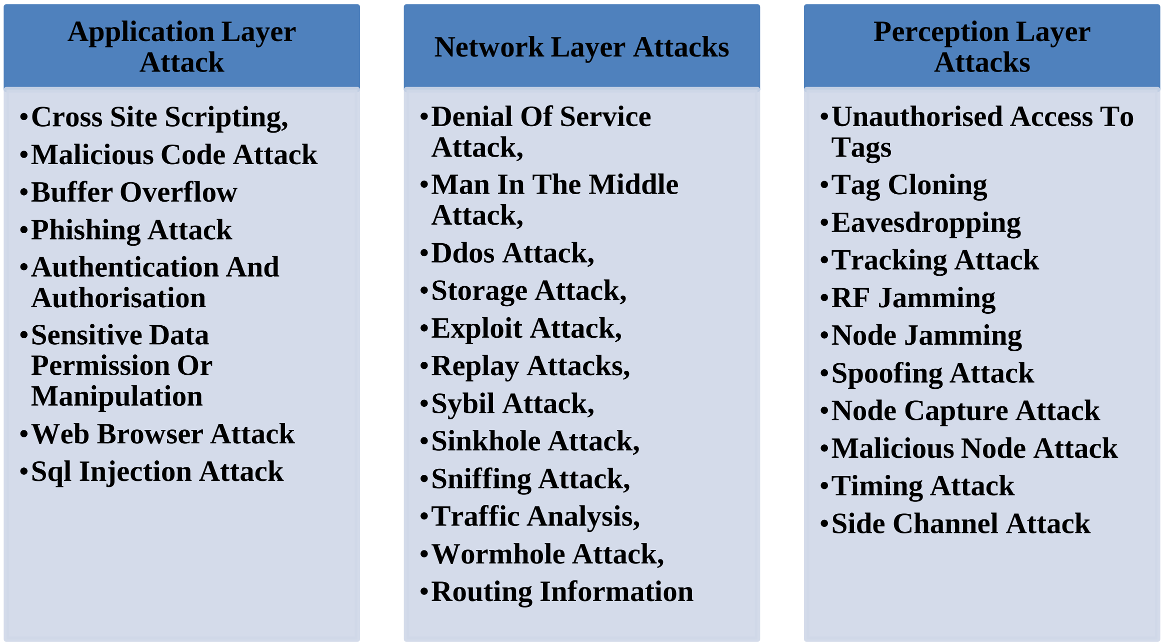

Fig.3. Taxonomy of Various Security Attacks in IOT based on Architecture Layers

3.1 **Perception Layer Attacks**

RFID systems do not have reliable authentication technologies, which allow unauthorized attackers to easily access tags [8, 9, 10]. Data can be abused by attackers. Once an intruder can reach the network, he can initiate the attack in wireless sensor networks or use the network free of cost.

Cloning of RFID tags is a successful attack. In order to do that, an assailant can get the details from reverse engineering or the operating environment directly [8, 11]. In previous work [8], for example, compromises were seen, since RFID readers can't say the difference between the tag and the tag.

In particular in wireless communications [8,11], the intruder will effectively eavesdrop the device and node of the sensor. An antenna can be used to record communications between legit tags and readers in an RFID system [12]. Unapproved users can, for example, use the antenna to catch information from reader to tag[13].

The system sends RF signals to avoid the communication of the legal tag to the readers[8, 13, 11, 14]. An intruder will use an RFID tag that prohibits readers from interacting with all tags to interact with all signals within their range [13]. The data collection mechanism on the awareness levels can be destroyed by this form of attack.

In any case, a tag that gains the same authorization or operation as a legitimate tag may be disguised as a valid one. They will then trick the reader to get the same authorizations as the legitimate tag. In earlier work[13], an intruder must have access and deep knowledge of protocols and automation in order to get the same authorization as the legitimate tag. The attacker must have access to the contact channel that is similar to the original tag. Notice that the loss of packet during the transmission procedure will result from spoofing attacks [15]. In addition, such an attack would force nodes to resend data, which would theoretically dramatically increase network traffic.

The strength of the battery restricts the device and the node of the vision layer. It is necessary for the system to sleep while not operating to extend its lifespan. This form of attack is intended to subvert this mechanism by sending control data to the system continuously and keeping the node running [8].

3.2 Network Layer Attacks

A denial-of-service attack (DoS attack) is executed in a network, causing a significant amount of network traffic to be created [8, 15, 16]. This kind of attack can deplete all available resources and prevent users from accessing network resources. Much user information that is not encrypted can even be leaked [8]. Moreover, the DDoS assault can incorporate multi-computer attacks as an attachment platform and operate on one or more targets with the start of DDoS.

In the Sybil attack, a device node includes numerous identities for the victim nodes, which helps the victim node to carry out an action twice, thus defeating redundancy [8, 15, 17]. The victim node can transfer information on through a compromised node that leads to a longer routing distance in the wireless network (WSN), since an attacker has multiple identities.

Attackers use the included node to pull data from the surrounding nodes in a sinkhole assault [8, 15, 18]. In [8], the device has been tricked and the data has been hit already. With WSN, a malicious node can be used by the assailant to draw network traffic and the sensor data can be randomly used [16].

In order to get information about the network and then steal useful data, attackers would be using sniffer devices and software [8, 10].

Attackers deduce communication pattern and load by observing data packet numbers and sizes [10, 19]. The more packets you can analyze, the more useful knowledge you can receive. This form of attack can be extended to encrypted packets. It is also possible to analysis the transmission pattern. Three forms of traffic monitoring can be used to collect data from WSN [38]. Next, the network behavior can be identified by an intruder. Secondly, an intruder can find wireless connection points physically (APs). Finally protocol style information used during the transmission process may be learned by an attacker.

Attackers are eavesdropping to collect information from the two parties. Received messages are regularly exchanged between communication pairs, which make communication services complicate. This assault also occurs with RFID technologies in reader-to-RFID-tag correspondence. The assault does not only absorb reader-to-tag computational resources but also takes backend database resources [11]. Apart from the above effects, reader access can be obtained by radio signal transmission.

In man in the middle attack, assault happens in real time between two victims' nodes. A legal node connecting with two victims nodes [8, 10, 20] is hidden by the perpetrator. Two nodes are comfortably collected and two victim nodes are identified.

3.3 Application Layer Attacks

Code Injection Attack requires malicious code being inserted into the device by using errors in software [8, 13]. Code injection can be used to steal data, gain power, and spread worms for a number of reasons, for example [12, 21]. Shell injection and HTML script injection are typical attacks. This form of attack can cause the system to lose control or even to shut down the whole system by jeopardizing user privacy.

Buffer flow attack requires an infringement of code or data buffer constraints by leveraging the limitations of the software. Variously, a memory structure is used to contain code and data fragments in a variety of applications. A long series of data is written to a given field by the attacker, leading to a sequence overflow past the predefined region of the home. This will result in altering other data (for instance where the series is intruding in the data field of another data buffer), malicious code execution (for example, code section prevention), and a software control flow destruction. Stack/heap buffer overload, string attack, integer error and double free [13, 22] are common approaches.

Protected information handling attacks relate to unauthorized and sensitive data access and handling, thereby breaching the privacy of consumers [23]. This attack generally takes advantage of implementation faults on the model authorization. In the model of permission to manage applications in smart homes, there has also been evidence of attackers exploiting vulnerabilities which cause problems such as theft and breakdown. In comparison, earlier work [24] studied SmartApp's and SmartDevice's activities. Notice that the issue of data protection lies with SmartApps and SmartDevices. A SmartDevice can send SmartApp critical data via events; SmartApp uses SmartDevice monitoring events. This, though, could lead to leaks of the event and much more significant damage to the consumer, due to the lack of adequate security for the event. Furthermore, since user input is not sufficiently protected, user privacy can be broken. A structure was proposed to secure confidential data by announcing expected data flow patterns in order to address the above issues.

In the phishing attack, an intruder appears to be a real person or a legal institution for confidential user details such as passwords and credit card information [8, 25]. The popular medium for this attack is an email, where a person has obtained private information before the email is opened.

In order to preserve IoT protection and privacy, the authentication function plays a key role. There can be no fine-grain checking of the new authentication schemes [26]. For eg, when installed, the applications can download malicious payloads, and attackers can use them to monitor a computer remotely [24]. In the meanwhile, the authorization model still includes vulnerabilities. Over privileges allow the device to access information without using all appropriate elements are a common problem [27]. In addition, an issue with the authorization source is also the default setting. In addition, an attacker can use this vulnerability to build attacks to varying degrees if a file and a directory are granted unauthorized permission. The smart card incorporates remote authentication vulnerabilities in a special application scenario considered in previous work that can allow user information to leak and be manipulated. Moreover, an intruder may carry out illegal activities, such as opening the door, due to the absence of a perfect security system in the smart home.

Web browser instructions, such as authentication and permission commands, are used by remote servers in the cloud [28]. But it's not possible for the browser itself to create XML tokens. Attackers take advantage of this vulnerability to obtain unidentified access. A web-based cloud services may create such metadata, containing a vast number of cloud-related content and the deployment of services. Once these metadata are obtained by attackers, they may pose a cloud threat [28].

A badly built software may be vulnerable to such attacks by inserting SQL statements into the input data [29]. For reading, write, and erase, attackers use these SQL statements. This method of attack not only helps the attacker to access private information, but also attacks the whole database structure. When SQL injection assaults on web apps, the present page reveals numerous findings compared with real information.

4. Conclusion

IoT technology has transformed people's lives due to the ability to gather information, connect and process. One of the main challenges to the advancement of the Internet-of-Things is protection and privacy. IoT attacks may constitute an invasion of privacy and may endanger the protection of people's lives and privacy. The security of the privacy of users has been another significant problem in the growth of IoT. A lot of study focuses on IoT protection and privacy, but the counter-measures discussed in these studies mostly concentrate on a single form of attack. It is also important to view the IoT architecture as a whole and to provide holistic security.

This paper addresses security risks and privacy issues in each layer of the IoT architecture. The IoT attack is assessed according to various classification criteria. At the same time, the protection of each layer on the IoT architecture should be enforced. Important more study is needed to establish a robust protection framework for the whole IoT architecture, including the implementation of intrusion detection systems and risk evaluation and mitigation.

References:

[1] Raghuvanshi, A., Singh, U. (2020). Internet of Things for smart cities- security issues and challenges. *Materials Today: Proceedings*. doi: 10.1016/j.matpr.2020.10.849

[2] Dunn JE. Wikipedia fights off huge DDoS attack; Sep 11, 2019. https://nakedsecurity.sophos.com/2019/09/11/wikipedia-fights-off-huge-ddos- attack/. Accessed September 18, 2019.

[3] World's largest DDoS attack: US firm suffers 1.7 Tbps of DDoS attack; March 6, 2018. https://www.hackread.com/worlds-largest-ddos-attack- us-firm-suffers-1-7-tbps-of-ddos-attack/. Accessed January 8, 2019.

[4] Osborne C. GitHub suffers “largest DDoS” attack in site's history; March 30, 2015. https://www.zdnet.com/article/github-suffers-largest-ddos- attack-in-sites-history/. Accessed January 8, 2019.

[5] Yang, Zhihong, et al. "Study and application on the architecture and key technologies for IOT." *Multimedia Technology (ICMT), 2011 International Conference on*. IEEE, 2011.

[6] Wu, Miao, et al. "Research on the architecture of Internet of Things." *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*. Vol. 5. IEEE, 2010.

[7] Saxena M. (2020). Novel framework and service model for internet of things in context of smart cities. International research journal of modernization in engineering technology & Science. 2(9), 1730-1735.

[8] Farooq MU, Waseem M, Khairi A, Mazhar S (2015) A critical analysis on the security concerns of Internet of Things (IoT). Int J Comput Appl 111:7

[9] Khan R, Khan S, Zaheer R, Khan S (2012) Future internet: the Internet of Things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology (FIT). IEEE, pp 257–260

[10] Welch D, Lathrop S (2003) Wireless security threat taxonomy. In: 2003 IEEE Systems, Man and Cybernetics Society and Information Assurance Workshop. IEEE, pp 76–83

[11] Ding Z-h, Li J-t, Feng B (2008) A taxonomy model of RFID security threats. In: 2008 11th IEEE International Conference on Communication Technology. ICCT 2008. IEEE, pp 765–768

[12] Yampolskiy M, Horvath P, Koutsoukos XD, Xue Y, Sztipanovits J (2013) Taxonomy for description of cross-domain attacks on CPS. In: Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems. ACM, pp 135–142

[13] Mitrokotsa A, Rieback MR, Tanenbaum AS (2010) Classification of RFID attacks. Gen 15693:14443

[14] Khoo B (2011) RFID as an enabler of the Internet of Things: issues of security and privacy. In: 2011 International Conference on Internet of Things (ithings/CPSCom) and 4th International Conference on Cyber, Physical and Social Computing. IEEE, pp 709–712

[15] Sastry AS, Sulthana S, Vagdevi S (2013) Security threats in wireless sensor networks in each layer. Int J Advan Netw Appl 4(4):1657

[16] Zhang W, Qu B (2013) Security architecture of the Internet of Things oriented to perceptual layer. Int J Comput, Consum Control (IJ3C) 2(2):37–45

[17] Douceur JR (2002) The Sybil attack. In: International Workshop on Peer-to-Peer Systems. Springer, pp 251–260

[18] Ahmed N, Kanhere SS, Jha S (2005) The holes problem in wireless sensor networks: a survey. ACM SIGMOBILE Mobile Comput Commun Rev 9(2):4–18

[19] Padmavathi DG, Shanmugapriya M et al (2009) A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv:0909.0576

[20] Cho J-S, Yeo S-S, Kim SK (2011) Securing against brute-force attack: a hash-based RFID mutual authentication protocol using a secret value. Comput Commun 34(3):391–397

[21] Mattern F, Floerkemeier C (2010) From the internet of computers to the Internet of Things, From active data management to eventbased systems and more, pp 242–259

[22] Zhu B, Joseph A, Sastry S (2011) A taxonomy of cyber attacks on SCADA systems. In: Internet of Things (Ithings/CPSCom), 2011 international conference on and 4th international conference on Cyber, Physical and Social Computing. IEEE, pp 380–388

[23] Jia YJ, Chen QA, Wang S, Rahmati A, Fernandes E, Mao ZM, Prakash A, Unviersity SJ (2017) ContexIoT: towards providing contextual integrity to appified IoT platforms. In: Proceedings of the 21st Network and Distributed System Security Symposium (NDSS'17)

[24] Fernandes E, Jung J, Prakash A (2016) Security analysis of emerging smart home applications. In: 2016 IEEE Symposium on Security and Privacy (SP). IEEE, pp 636–654

[25] Thakur BS, Chaudhary S (2013) Content sniffing attack detection in client and server side: a survey. Int J Advan Comput Res 3(2):7

[26] Simmons C, Ellis C, Shiva S, Dasgupta D, Wu Q (2009) AVOIDIT: a cyber attack taxonomy

[27] Bugiel S, Heuser S, Sadeghi A-R (2013) Flexible and fine-grained mandatory access control on Android for diverse security and privacy policies. In: USENIX Security Symposium, pp 131–146

[28] Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On technical security issues in cloud computing. In: 2009 IEEE International Conference on Cloud Computing. CLOUD'09. IEEE, pp 109–116

[29] Zhang Q, Wang X (2009) SQL injections through back-end of RFID system. In: 2009 International Symposium on Computer Network and Multimedia Technology. CNMT 2009. IEEE, pp 1–4