Internet of Things:Threats and Security Attacks, Counter Measures and Challenges

Angelin JL[1] ,Dr.V.Nethaji[2], & DM Sheeba[3]

1,Dept of Computer Scienc, New Prince Shri Bhavani Arts & Science College,Chennai, jlangelincharles@gmail.com

2, *Dept of Computer Scienc, New Prince Shri Bhavani Arts & Science College,Chennai,sivakami03@yahoo.com*

3, Dept of Computer Scienc, New Prince Shri Bhavani Arts & Science College,Chennai,sheebadm@gmail.com

***Abstract*—Internet of Things (IoT) is an embedded technology which emphasis interconnecting of different electronic devices through network. However, during the past decade IoT has rapidly been developed without appropriate consideration of the profound security goals and challenges involved. This study explores the security aims and goals of IoT and then provides a new classification of different types of attacks and countermeasures on security and privacy. This paper also forecast the key challenges associated with the development of IoT. It then discusses future security directions and challenges that need to be addressed to improve security concerns over low powered IoT devices.**

Keywords—Internet of Things, attacks, vulnerabilities, security challenges.

I. INTRODUCTION

Internet of Things allows electronic devices by sharing information with other members of the network making it possible to recognize events and changes in their surroundings and to act and react autonomously mainly without man-man communication rather than machine–machine communication[1] . The advantages of IoT are almost limitless and its applications are changing the way we work and live by saving time and resources, and opening new opportunities for growth, innovation, and the exchange of knowledge between entities. However, the existence of such a large network of interconnected entities will definitely pose new security, privacy, and trust threats that put all those devices at a high risk, thus harming the affiliated users.

This paper represents the IoT architecture and components. Then it explores the IoT security goals and the literature review of the work done on security of IoT[2]. It provides a classification of the security challenges in IoT Systems. Then it establishes new security directions to countermeasure and threats.

II. IOT OVERVIEW

The Internet of Things has been evolved into a reality that interconnects real world sensors, electronic devices and systems to the Internet such as Consumer services, smart houses, and smart objects, Smart energy, smart meters and grids Smart phones and Tablets, Internet connected cars, Wearable devices; health and fitness monitoring devices, watches, smart clothing, pets smart collars or implanted RFIDs, and even human implanted devices (pacemakers), [3]Wireless sensor networks, weather measuring, health care monitoring, industrial monitoring, data loggings, environmental monitoring (water quality, earth sensing fire detection, air pollution monitoring) etc.

A. Technologies in IOT

IoT is implemented using a variety of existing network technologies, and more specifically using the following three:

1) RFID

Radio Frequency Identification technology enables the design of microchips for transmitting data in wireless data communication.[4] They use tags (labels) attached on objects for automatic identification acting as electronic barcodes.

2) WSN

Wireless Sensor Networks . A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes.

B. IoT Architecture

The following diagram represents the structure of IoT which includes gateways, cloud infrastructures, network infrastructures and the communicating devices.

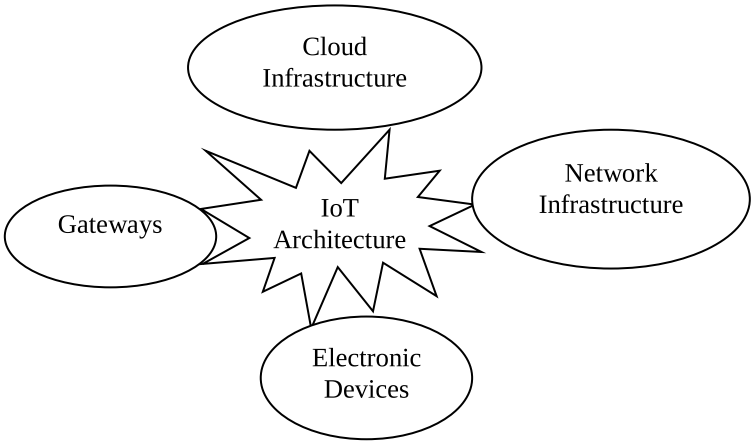

Fig. 1. IoT Architecture

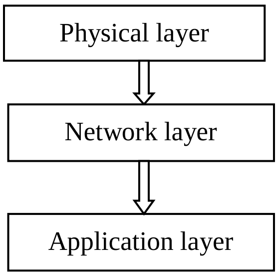

Fig 2. Layers of Iot Architecture

A. *IoT Protocols(TCP/IP):*

The architecture of an IoT system is similar to that of the TCP/IP Stack, it does not use the same protocols at the different layers because of the low power devices that are present in the IoT and their required operation of months or years without getting any power recharge. Therefore, less power equals to less computation power available to the devices; hence standard TCP/IP protocols become less ideal and suboptimal for the IoT characteristics and challenges[5]. This raises security concerns as the interoperable IoT protocols and open IoT standards lack the security foundation compared to the TCP/IP Stack protocols.

B. *Physical Layer*

The bottom layer of the architecture is basically the layer responsible for the interconnected devices and its main purpose is to perform device identification and provide service discovery[6]. These devices can be of various types (Arduino, Raspberry, ZigBee, etc.), but in order to be considered as IoT devices they need to utilize communication technology that allow them to connect to one another either directly or indirectly using the Internet; e.g., Arduino with Ethernet connection, a Raspberry Pi with a Wi-Fi connection, a Bluetooth connection, and a low power radio connection.

C. *Network Layer*

Like any other Network Layer model this one includes network interfaces, communication channels, network management, information maintenance, and intelligent processing, and is mainly responsible for the communication and connectivity of all the devices in IoT system through the help of multiple communication protocols [7].

D. *Application Layer*

This layer is service-oriented which ensures the same type of service among the connected devices. It can store data into a database providing storage capabilities to the collected data. Also, just like its name suggests, it facilitates ways for these devices to communicate outside of the device-oriented system with the use of different kind of applications depending on the needs of the users [8]; e.g., Smart Home, e-Health, Smart Transportation, Smart Objects etc.

III. CLASSIFICATION OF IOT SECURITY ATTACKS

The classification of IoT paper attempts to capture a broader spectrum of the security vulnerabilities and attacks in IoT systems. Our classification is unique compared to other classifications as it divides the different attacks under four distinct classes; Physical, Network, Software and Encryption attacks[9][10][11][12]. An IoT system can be attacked physically, or attacked from within its network, or from applications on the system, and lastly from attacks on encryption schemes[13]. A summary of the classification of the attacks is shown in Table 1 below.

Table I. VARIOUS TYPES OF IOT ATTACKS

<table>
<tr><th>Physical Attacks</th><th>Network Attacks</th><th>Software Attacks</th><th>Encryption Attacks</th></tr>
<tr><td>Node Jamming</td><td>RFID Cloning</td><td>Spyware and Adware</td><td rowspan="6">Cryptanalysis Attacks:
a) CipherText attack Only
b) Known Plain Text attack
c) Choose Plain Text (or) Cipher text Attack</td></tr>
<tr><td>Malicious Node Injection</td><td>RFID Unauthorised Access</td><td>Spyware and Adware</td></tr>
<tr><td>Physical Damage</td><td>Sinkhole Attack</td><td>Trogen Horse</td></tr>
<tr><td>Social Engineering</td><td>Man In the Middle Attack</td><td>Trogen Horse</td></tr>
<tr><td>Node Tampering</td><td>Traffic Analysis Attacks</td><td>Virus and worms</td></tr>
<tr><td>RF Interference</td><td>RFID Spoofing</td><td>Virus and worms</td></tr>
<tr><td>Sleep Deprivation Attack</td><td>Denial of Service</td><td>Malicious scripts</td><td rowspan="3">Man In The Middle Attack</td></tr>
<tr><td rowspan="2">Malicious Code Injection on the Node</td><td>Routing Information Attacks</td><td rowspan="2">Denial of Service</td></tr>
<tr><td>Sybil Attack</td></tr>
</table>

A. *Network Attacks*

These attacks are centred on the IoT system network and the attacker does not necessarily need to be close to the network for the attack to work.

1) *Traffic Analysis Attacks*

An attacker can sniff out the confidential information or any other data flowing from the RFID technologies because of their wireless characteristics [14]. Also, in almost all of the attacks an attacker first tries to gain some network information before he employs his attack. This is done using sniffing applications like port scanning application, packet sniffer applications etc. [15][16][17].

2) *RFID Spoofing*

An attacker spoofs an RFID signals to read and record a data transmission from an RFID tag[19][20]. Then the attacker can send his own data containing the original tag ID, making it appear to be valid, hence the attacker gains full access to the system pretending to be the original source [18].

3) *RFID Cloning*

An attacker clones an RFID tag by copying data from the victims RFID tag, onto another RFID tag[21]. Although the two RFID tags have identical data, this method does not replicate the original ID of the RFID, making it possible to distinguish between the original and the compromised, unlike the event in the RFID spoofing attack[22]-[28].

4) *RFID Unauthorised Access*

Because of the lack of proper authentication mechanisms in the majority of RFID systems, tags can be accessed by anyone. This automatically means that the attacker can read, modify or even delete data on the RFID nodes [29].

5) Sinkhole Attack

The attacker lures all traffic from WSN nodes, hence creating a metaphorical sinkhole. This type of attack breaches the confidentiality of the data and also denies service to the network by dropping all the packets instead of forwarding them to the desired destination [30].

6) Man In the Middle Attack

The attacker over the network manages to interfere between two sensor nodes, accessing restricted data, violating the privacy of the two nodes by monitoring, eavesdropping and controlling the communication between the two sensor nodes [31]. Unlike the Malicious Node Injection from the Physical Attacks category, the attacker does not necessarily need to be physically there for this kind of attack to be successful, but relies solely on the network communication protocols of an IoT system.

7) Denial of Service

An attacker can bombard an IoT network with more traffic data that it can handle which can result in a successful Denial of Service attack

8) Routing Information Attacks

These are direct attacks that the adversary by spoofing, altering or replaying routing information can complicate the network and create routing loops, allowing or dropping traffic, sending false error messages, shortening or extending source routes or even partitioning the network [30]; e.g. Hello Attack [31] and Blackhole Attack.

9) Sybil Attack

A malicious node (i.e. Sybil Node), is a single node that claims the identities of a larger number of nodes, and impersonating them. This kind of attack leads to false information being accepted by the neighbouring WSN nodes; e.g. imagine a WSN voting system where one Sybil node votes more than once [25], or a Sybil node being selected as part of a routing path.

B. Software Attacks

Software attacks are the main source of security vulnerabilities in any computerised system. Software attacks exploits the system by using Trojan horse programs, worms, viruses, spyware and malicious scripts that can steal information, tamper with data, deny service and even harm the devices of an IoT System.

1) Phishing Attacks

The attacker gains access to confidential data by spoofing the authentication credentials of a user, usually through infected emails or phishing web sites [26].

2) Virus, Worms, Trojan Horse, Spyware and Aware

An adversary can infect the system with malicious software resulting in a variety of outcomes; stealing information, tampering data or even denial of service [27].

3) Denial of Service

An attacker can execute DoS or distributed denial of service DDoS attacks on the affected IoT network through the application layer, affecting all users in the network. This kind of attack can also block the legitimate users from the application layer giving full application layer access to the attacker; databases and private sensitive data [28].

C. Encryption Attacks

These attacks are solely based on breaking the encryption scheme being used in an IoT system.

1) Side channel Attacks

Using particular techniques (i.e. Timing, Power, Fault and Electromagnetic Analysis) on the encryption devices of an IoT system, the attacker can retrieve the encryption key being used for encrypting and decrypting data.

2) Cryptanalysis Attacks

These attacks assume the possession of ciphertext or plaintext and their purpose is to find the encryption key being used by breaking the encryption scheme of the system. Examples of cryptanalysis attacks on IoT systems include Known-plaintext attack, Chosen-plaintext attack, Chosen Ciphertext attack, and Ciphertext-only attack.

3) *Man In the Middle Attack*

When two users of an IoT system A and B, exchange keys during a challenge-response scenario, so as to establish a secure communication channel, an adversary positions himself between them on the communication line. The adversary then intercepts the signals that A and B send to each other and attempt to interfere by performing a key exchange with A and B separately. The adversary will then be able to decrypt/encrypt any data coming from A and B with the keys that he shares with both of them. Both A and B will think that they are talking with each other.

IV. SECURITY GOALS

Because IoT is a relatively new concept, there is a need to define its security goals. To successfully achieve this we need to understand that IoT is an implementation of network technologies and an integration of existing network infrastructures (e.g. wireless sensor networks, RFIDs based sensor networks, Cloud Computing, the Internet etc.). Therefore, all of the security challenges and threats of each network technology are passed by default onto the IoT system that utilises these technologies. Further, there is the possibility of additional security threats that arise from the coexistence and collaboration of the different technologies and the open standards and protocols created for the IoT. The most desirable security objective of IoT is to protect the collected data, since the data collected from physical devices may also include sensitive user information. For this reason the security of any IoT system needs to be resilient to data-related attacks and provide trust and data security and privacy.

A. *Security and Privacy in IoT Definition*

In this paper data security and privacy refers to the protection of any collected or stored data in any IoT system. This means that at any moment the IoT system needs to provide data confidentiality, integrity, and availability. This can be achieved by utilizing authentication, access control, data encryption, and data availability and redundancy through back-ups and etc.

Security architecture for the IoT based on their security challenges and goals. Although there has been work on the security of RFID systems and Wireless Sensor

V. SECURITY FUTURE DIRECTIONS

In this Section we will provide future directions for security based on the challenge classification presented earlier. An IoT system consists of three different layers each with vulnerabilities and security attacks.

To address these attacks and to successfully protect the IoT system, this section presents a multi-layered security approach that should be structured to give an optimal layered protection at each layer in an IoT system as shown on the next page in Table II. A detailed description of the table is explained below.

A. *IoT Physical Layer Security*

a) Device authentication: When a new device is introduced to the network, it should authenticate itself before receiving or transmitting data, to ensure it is identified correctly before authorization and keeping malicious devices out of the system.

b) Data integrity: Error detection mechanisms should be provided at each device, to ensure no tampering of sensitive data occurs. Low power consumption mechanisms like Cyclic Redundancy Checks (CRC), Checksum, Parity Bit are preferred.

c) Data Confidentiality: All RFID Tags, IDs and data should be encrypted on each device before transmission of data to ensure confidentiality. However, because of the ultra- low power consumption, strong cryptographic encryption functions like AES cannot be implemented. Instead Blowfish or RSA have lower power consumption and less processing power and can be successfully implemented on the physical layer devices.

B. *IoT Network Layer Security*

a) Data privacy: Illegal access to the sensor nodes can be prevented, using authentication mechanisms and point to point encryption [29].

b) Data integrity: Using cryptographic hash functions, the integrity of the data received on the other end is confirmed. In case of prove of tampering of data, error correction mechanisms could be introduced to mitigate the problem.

C. *IoT Application Layer Security*

a) Data security: Authentication Encryption and Integrity mechanisms are critical at this level for insuring the privacy of the whole system and protecting against data theft; it prevents unauthorised access to the system and ensures the confidentiality of the system data.

b) Access Control Lists (ACLs): Setting up policies and permissions of who can access and control the IoT system, is a crucial part as this ensures the privacy of the data, and the well being of the system. ACLs can block or allow incoming or outgoing traffic, and give or block access to requests from different users inside or outside of the network.

c) Anti-virus, Anti-spyware and Anti-adware: Security software like antivirus or anti spyware is important for the reliability, security, integrity and confidentiality of the IoT system.

To insure the continued protection of an IoT system and maintain its trustworthiness, Risk Assessment, Intrusion Detection, Physical Security and Trust Management should be mandatory at all layers in IoT.

VI. CONCLUSION

Though a lot of companies state that their technologies are secured and protected, they are still prone to various types of attacks. Since the interconnected devices have a direct impact on the lives of users, there is a need for a well-defined security threat classification and a proper security infrastructure with new systems and protocols that can mitigate the security challenges regarding privacy, data integrity, and availability in IoT.

Due to its rapid progression many threats in security and privacy exists, which hinder its development. This paper explored the security goals required for a secure IoT system, and classified its security challenges and issues using a new unique classification method consisting of four classes of attacks; Physical, Network, Software, and Encryption Attacks. Based on this classification, we then highlighted the security countermeasures needed to successfully secure an IoT system. Furthermore, future directions for security for IoT were discussed. This classification could be used as a framework to categorize attacks, as well as to guide the secure deployment of IoT systems. As future work, we aim to investigate the interaction.

REFERENCES

[1] M. Feldhofer, and C. Rechberger, "A case against currently used hash functions in RFID protocols." In On the move to meaningful internet systems 2006: OTM 2006 workshops, pp. 372-381. Springer Berlin Heidelberg, 2006.

[2] J. P. Kaps, "Cryptography for ultra-low power devices." PhD diss., WORCESTER POLYTECHNIC INSTITUTE, 2006.

[3] U. Feige, F. Amos, and S. Adi,. "Zero-knowledge proofs of identity." Journal of cryptology 1, no. 2 (1988): 77-94.

[4] L. Sweeney, "k-anonymity: A model for protecting privacy." International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10, no. 05 (2002): 557-570.

[5] G. Peretti, V. Lakkundi, M. Zorzi, "BlinkToSCoAP: An End-to- End Security Framework for the Internet of Things." (2015).

[6] X. F. Wang, "Research on Security Issues of the Internet of Things." InAdvanced Materials Research, vol. 989, pp. 4261-4264. 2014.

[7] Z. Xu, Y. Yin, and J. Wang, "A density-based energy-efficient clustering algorithm for wireless sensor networks." International Journal of Future Generation Communication and Networking 6, no. 1 (2013): 75-86.

[8] C. Liu, Y. Zhang, J. Zeng, L. Peng, and R, Chen, "Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology." In Natural Computation (ICNC), 2012 Eighth International Conference on, pp. 874-878. IEEE, 2012.

[9] A. Patcha, and J. M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends." Computer Networks 51, no. 12 (2007): 3448-347.

[10] D. Chen, G. Chang, D. Sun, J. Li, J. Jia and X. Wang "TRM-IoT: A trust management model based on fuzzy reputation for internet of things." Computer Science and Information Systems 8, no. 4 (2011): 1207-1228.

[11] F. Bao and I. Chen, "Trust management for the internet of things and its application to service composition", in Proc. of IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012, pp.1-6.

[12] F. Bao, I. Chen and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems", in Proc. of IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), (2013), pp.1-7.

[13] M. Nitti, R. Girau, L. Atzori, A. Iera and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of Things", in Proc. of IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), (2012) pp. 18-23.

[14] Y. Liu and K. Wang, "Trust control in heterogeneous networks for Internet of Thing", in Proc. of International Conference on Computer Application and System Modeling (ICCASM), (2010), pp.632-636.

[15] D. Gessner, A. Olivereau, A.S. Segura and A. Serbanati, "Trustworthy infrastructure services for a secure and privacy-respecting internet of things", in Proc. of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), (2012) pp.998-1003.

[16] Z. Yan, P. Zhang, A. V. Vasilakos, "A survey on trust management for Internet of Things." Journal of network and computer applications 42 (2014): 120-134 [19] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29, no. 7 (2013): 1645-1660.

[17] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)." Perception 111, no. 7 (2015).

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

[19] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID attacks." Gen 15693 (2010): 14443.

[20] M. Burmester, and B. De. Medeiros, "RFID security: attacks, countermeasures and challenges." In The 5th RFID Academic Convocation, The RFID Journal Conference. 2007.

[21] R. Uttarkar, and R. Kulkarni, "Internet of Things: Architecture and Security."

[22] L. Li, "Study on security architecture in the Internet of Things." In Measurement, Information and Control (MIC), 2012 International Conference on, vol. 1, pp. 374-377. IEEE, 2012.

[23] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks." Communications of the ACM 47, no. 6 (2004): 53-57.

[24] V. Soni, P. Modi, and V. Chaudhri, "Detecting Sinkhole attack in wireless sensor network." International Journal of Application or Innovation in Engineering & Management 2, no. 2 (2013).

[25] D. Wu, and G. Hu, "Research and improve on secure routing protocols in wireless sensor networks." In Circuits and Systems for Communications, 2008. ICCSC 2008. 4th IEEE International Conference on, pp. 853-856. IEEE, 2008.

[26] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud Computing: Security Issues and Research Challenges." International Journal of Computer Science and Information Technology & Security (IJCSITS) 1, no. 2 (2011): 136-146.

[27] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses." In Proceedings of the 3rd international symposium on Information processing in sensor networks, pp. 259-268. ACM, 2004.

[28] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs." Communications Surveys & Tutorials, IEEE 11, no. 4 (2009): 42-56.

[29] M. A. Hamid, M. Mamun-Or-Rashid, and C. S. Hong, "Routing security in sensor network: Hello flood attack and defense." IEEE ICNEWS (2006): 2-4.

[30] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing." Communications of the ACM 50, no. 10 (2007): 94-100.

[31] B. S. Thakur, and S. Chaudhary, "Content sniffing attack detection in client and server side: A survey." International Journal of Advanced Computer Research (IJACR) 3, no. 2 (2013): 10.