Information Security in Internet of Things: A Review

Prof. Dr. Nitin N. Patil, Makarand L. Mali

Department of Computer Engineering, R. C. Patel Institute of Technology, Shirpur
er.nitinpatil@gmail.com, malimakarand1@gmail.com

Abstract

The interactive and communicating collaboration among sensors, nodes actuators, microcontrollers and mobile devices is the formation of an advanced computing technology called as Internet of Things. These IoT devices can help to improve each aspect of human life based on information processing. Currently a huge number of IoT devices communicate via Internet and this number is increasing rapidly day by day as in various attempts to improve our lives with better safety and comfort. All these devices process the huge amount of information obtained from Internet, sensors, microcontrollers or other IoT devices with 'command and control' action. This paper comprises a review of necessity of information security in IoT. The information security is a crucial issue which requires proper attention if not can affect the escalation of IoT.

Keywords: *Information, Security, Internet of Things, IoT*

1. Introduction

Human to human communication is most widely preferred than the human to things and things to things. Here things mean devices like sensors, actuators, microcontrollers etc. These things are heart of the Internet of Things technology. Therefore, the IoT domain consists of devices and human interactions. If we consider interactive word, then there is communication with the help of digital information. This digital information may hold confidential data, passwords, IDs, usernames etc. This big data moving around the world through the Internet. There is more than fifty million IoT devices communicating over the Internet today. Thus, a lot of information transfer from device to device and device to human or vice versa as we live in the world where everything is being connected through the Internet. Here we focus on the information security, which is in communication through IoT devices. Till now, very less work is done in context of information security in IoT and it is needed to be focused more. The rapidly expanding scope of IoT may also threat the information security in many ways. Some adversary intentionally breaches the information security in the IoT. To overcome these issues various researchers have contributed their efforts to make these communications secure. Our paper reviews different attempts introduced for information security mechanisms in IoT.

2. Vision of IoT

IoT is network of physical devices like vehicles, home appliances, machines, robots, industry or office appliances etc. These all appliances or devices communicate via Internet. Information is gathered from various sensors, microcontrollers, actuators and the appropriate processing takes place accordingly. This pre-processing and post processing of information is stored in the clouds. The cloud information maintenance is done by the cloud service providers. The definition of IoT may vary according to the researcher to researcher, book to book or application to application. As per our study and observation, we define the IoT as effective way of making human life easier.

The rapid growth of Internet enabled devices, ranging from sensors to highly complex servers, shape the Internet of Things world, where Things, in this context, refers to a wide

variety of objects. The similarity between all IoT objects is the ability to connect to the Internet and exchange data and communicate with the help of digitally secured information channels. The network connectivity leads to controlling things remotely. This connectivity includes infrastructure and resulting in better integration with the real world but through less human intervention. The IoT transforms these things from classical to smart by its underlying featured technologies such as pervasive computing, communication capabilities, Internet protocols and applications. The protocols are required to identify the digital information communicated during the IoT devices in terms of the format of messages and select the correct boundaries that comply with the functionality of each IoT device. The applications determine granularity and specialty of the IoT device and how big is the data generated for analysis. They also indicate the general context of the IoT framework used in the applied domain. The concept of IoT framework involves identifying an infrastructure which coordinates, monitors and controls processes conducted by the various IoT devices. This includes protocols where the protocols are the set of rules, and regulations that organize the processing of data and exchange of messages between things [22].

3. Possible Attacks on IoT

This section describes various possible attacks on IoT system. The nature of attack varies according to targeted element of an IoT system.

3.1 Physical Attacks:

Physical attacks are concentrated on hardware devices in the system.

1) Node Tampering: In this attack attacker physically alters the compromised node and can obtain sensitive information such as encryption key [1].
2) RF Interference on RFIDs: The attacker performs Denial of service attack by sending noise signals over radio frequency signals. These signals are used for RFID's communication [2].
3) Node Jamming in WSNs: By using jammer, the attacker can disturb the wireless communication. It causes Denial of service attack [1].
4) Malicious Node Injection: In this attack, attacker physically injects a new malicious node between two or more nodes. It then modifies the data which passes the wrong information to the other nodes. The attacker uses the multiple nodes to perform malicious node injection attack [3]. The adversary first inserts a replica of the node (e.g. Node B). After that, it inserts other malicious nodes (like node M1). Both these nodes work together to execute the attack. Thus the collision occurs at the victim node. Because of these, the attacked node cannot receive/send any packet. Hence, the conclusion of watchdog nodes might be affected by incorrectly announcing the attacked node (the legitimate node) as acting maliciously. To prevent this attack, we use a monitoring verification (MOVE) scheme. It can check the monitoring node(s) result and correctly identify any malicious behaviour. According to the acknowledgment, the verifier node will decide whether the node is malicious or not.
5) Physical Damage: The attacker physically harms components of IoT system and it results in Denial of service attack [4].
6) Social Engineering: The attacker physically interacts and manipulates users of an IoT system. The attacker obtains sensitive information to achieve his goals [4].
7) Sleep Deprivation Attack: The aim of the attacker is to use more power that results in shutting down of nodes [5].
8) Malicious Code Injection: The adversary physically introduces a malicious code into the node of IoT system. The attacker can get full control of IoT system [5].

3.2 Network Attacks:

These attacks are related to the network of IoT system.

1) Traffic Analysis Attacks: The attacker intercepts and examines messages to obtain network information [1].

2) RFID Spoofing: An adversary spoofs RFID signals. Then it captures the information which is transmitted from a RFID tag. Spoofing attacks give wrong information which seems to be correct and that the system accepts [2].
3) RFID Cloning: In this attack, adversary copying data from pre-existing RFID tag to another RFID tag. It does not copy original ID of RFID tag. The attacker can insert wrong data or control the data passing via the cloned node [6].
4) RFID Unauthorized Access: If the correct authentication is not provided in the RFID systems, then the adversary can observe, alter or remove information on nodes [6].
5) Sinkhole Attack: In a sinkhole attack an adversary compromises a node inside the network and performs the attack by using this node. The compromised node sends the fake routing information to its neighbouring nodes that it has the minimum distance path to the base station and then attracts the traffic. It can then alter the data and also drop the packets. A simple technique is proposed to identify sinkhole nodes. In proposed technique, when a node send a packet to its neighbouring node it creates the entry of hop distances and ID in its database. It then computes the average hop-count except minimum hop-count and compares average and minimum value. If this minimum value is too small as compared to the average hop-count, then it is vulnerable to sinkhole attack [7].
6) Man in the Middle Attacks: The attacker over the internet intercepts the communication between the two nodes. They obtain the sensitive information by eavesdropping [6].
7) Denial of Service: An attacker floods the network with large traffic so that services are unavailable to its intended users [8].
8) Routing Information Attacks: In this attack, the attacker can make the network complex by spoofing, modifying or sending routing information. It results in allowing or dropping packets, forwarding wrong data or partitioning the network [4].
9) Sybil Attack: In this attack, malicious node that takes the identities of multiple nodes and acts as them. In Wireless Sensor Network, voting system single node can vote many times [5].

3.3 Software Attacks:

The attacker performs the attack by using virus, worm, spyware, adware to steal data or to deny the services and so on.

1) Phishing Attacks: The attacker obtains the private information like username, passwords by email spoofing and by using fake websites.
2) Virus, Worms, Trojan horse, Spyware and Aware: An adversary can damage the system by using malicious code. These codes are spread through email attachments, downloading files from the Internet. The worm has the ability to replicate itself without any human action. We can use worm detector, anti-virus, firewalls, intrusion detection system to detect the virus. The paper [21] combines anomaly and signature detection with honeypot to protect the system from worms. This hybrid scheme takes the advantage of honeypot and anomaly/signature detection and provides the protection against worms.
3) Malicious Scripts: By injecting malicious script the attacker can gain access to the system.
4) Denial of Service: The attacker blocks the users from the application layer by denying services [4].

3.4 Encryption Attacks

These attacks depend on destroying encryption technique and obtain the private key.

1) Side-channel Attacks: The attacker uses the side channel information that is emitted by encrypting devices. It is neither the plaintext nor the cipher text, it contains information about power, the time required to perform the operation, faults frequency etc. Attacker uses this information to detect the encryption key. There are different types of side-channel attack such as timing attacks, Simple and Differential Power Analysis and Differential Fault Analysis Attacks. The timing attacks are dependent on the time require for executing operations. It gives the information of the secret keys. By using this information an attacker can find fixed Diffie-Hellman exponents, factor RSA keys and break other cryptosystems [9]. Cryptosystems process different inputs in different time. Because of branching and conditional statements, RAM cache hits, processor instructions that run in non-fixed time, etc. Timing computations are providing to a statistical model. It provides the guessed key bit to a certain extent of assurance. Cryptanalysis of a Simple Modular Exponentiation: Diffie-Hellman and RSA operations involve calculation of R = y mod n, where n is public and y can be obtained by a listener. The adversary wants to

search the secret key x. To perform the attack, the victim must calculate yx mod n for many values of y, where y, n and the estimation time are known to the adversary and x remains the same. The needed data and timing computation might be gained by secretly listening on an interactive protocol. Hence, an adversary could see the messages received by the target and calculate the time required to respond to each y. A common method to stop timing attacks is to perform all operations in such a way that they take absolutely the same amount of time by adding delay. Sometimes this is difficult.

2) Cryptanalysis Attacks: In this attack, the adversary obtains the encryption key by using either plaintext or ciphertext. Based on methodology used, there are different types of cryptanalysis attacks [6].
    a. Ciphertext Only Attack: In this the attacker can access the ciphertext and determine the corresponding plaintext.
    b. Known Plaintext Attack: In this method, the attacker knows the plaintext for some parts of the ciphertext. The aim is to decrypt the remaining part of the ciphertext utilizing this information.
    c. Chosen Plaintext Attack: The attacker gets to choose what plaintext is encrypted and find the encryption key.
    d. Chosen Ciphertext Attack: By using the plaintext of chosen ciphertext the attacker can find the encryption key [9].

The Man in the Middle Attacks: When two users are interchanging the key the attacker intercepts the communication and obtains the key [5].

4. Review of IoT Security

The IoT is known for emerging global Internet oriented information architecture smoothing the exchange of services. The IoT has the determination of providing an IT-infrastructure facilitating the exchange of information through the “things” in a secure and reliable manner. The IoT will serve to increase transparency as well as enhance the efficiency of supply of information.

Wide-ranging distribution of IoT devices and unsecured nature of data that are communicated by IoT devices made the major security challenge.

Authentication allows integration of different IoT devices which are deployed in various contexts in the digital world. This process involves authentication of IoT devices that transferring data from device to device or system to system. Authorization this property involves rights to access different resources or data within IoT. Every IoT device is responsible for inadequate mechanisms for access [10].

To challenge insufficiency of security IoT systems this work introduced a new design methodology for security IoT system. They proposed Security Framework for Internet of Things. And this framework suitable for forthcoming implementations and research. They compared the cryptography algorithms against various attacks and design algorithms [11]. The framework of the smart home system is also proposed and implemented the security, privacy protection based on the design of hardware and software [12].

To help the researcher the taxonomy of IoT authentication protocols is presented by comparing and classifying other authentication schemes. In addition, an analysis of the most known authentication mechanisms is summarized via a table of comparison.

The data analysis done on a cyber-physical system utilizing IoT for monitoring the quality of service. Instead of assuming security of the IoT device data, they have assessed the possible actions to be taken by malicious users for possible mitigation techniques, deciding on SHA hashing for the protection of riders’ privacy [13].

The HAN algorithm with a combination of AES symmetric encryption algorithm and NTRU asymmetric encryption algorithm for IOT improvement proposed. This algorithm has very high speed for to create a key, encryption and decryption and also acceptable security in IOT. The multinomial use of encryption, decryption with the benefit of digital signature is used to achieve a correct message as IoT security [14].

The IoT devices used to build the system are extremely tough, portable, easily available and affordable commercial used. The research work, particularly aims at creating a system which would detect motion as well as notify the user whether they are in any part of the world [15]. Internet of Things (IoT) plays a significant role in a healthcare domain, from tracking and monitoring diseases at one end to prevent diseases. This requires IoT sensors to gather information and uses gateway devices to analyse and store. Then send the information for analysis through

wireless medium to healthcare service providers for further decision making. These applications will improve the access to care by reducing the cost of care [16].

The growth of IoT is increasing day by day and the security and privacy requirements are also varying. The encryption, decryption techniques or cryptographic techniques are inadequate to fulfil the required security issues. Therefor, there is need of trivial and novel encryption techniques to overcome future needs. Although various in the research areas lightweight protocols are suggested, but it seems to be insufficient the field [17].

One of the researchers proposed secure MQTT protocol. In this protocol there are three things first is publisher device publishes the data, second thing is subscriber device receives the data and finally is the trusted third party. There are few phases in the protocol. In the first phase, registration and key management are initiated. During second one encryption phase, data is encrypted and in third phase i.e. publish phase, the publisher publishes encrypted data and sends it to the third party [18].

The [19] proposed IoT architectures for different layers, such as for the man in the middle attacks, spoofing, unauthorized access to private data. There will be universal standards in architecture, protocol, security and privacy requirements. New security protocols are used to resist network layer attacks, Cryptography algorithms and key management schemes effectively in IoT devices. Further these can promote the development and adoption of IoT technology.

An IoT architecture based on the 'MobilityFirst' network was proposed by Liu et al. This approach addresses security concerns and increases confidence about the assured operation of the Internet of Things. They introduced a layer in the architecture, which refer to as the IoT middleware that connects devices in local IoT systems to the global 'MobilityFirst Network'. The main devices of the IoT middleware is the IoT-NRS (IoT name resolution service), which is a device registering service that provides identification and key management.

The recent Internet security protocols depend on a well-known and widely trusted suite of cryptographic algorithms. The Advanced Encryption Standard (AES) block cipher is used for secrecy, the Rivest-Shamir-Adelman (RSA) asymmetric algorithm is used for digital signatures and key transport, the Diffie-Hellman (DH) asymmetric key agreement algorithm and the SHA- 1 and SHA-256 can be used as secure hash algorithms. These all packages of algorithms are enhanced by a set of emerging asymmetric algorithms, known as Elliptic Curve Cryptography (ECC).

9. Conclusions

Providing security for IoT technology is really challenging, mainly because there is not any boundary or limitation on the extent that it can be developed to in the future. In this paper, we reviewed the possible challenges, architectures algorithms as well as the method to provide security in IoT. In this paper, we have tried to highlight threats to the IoT systems by citing studies of some of the successful security concerns. Also, some open research challenges or issues related to IoT information security were discussed. The future work of this research will be evaluation of diversities in IoT information security to both hardware and software.

References

10.1. Journal Article

[1] S.N Uke, A.R Mahajan, R.C Thool *"UML Modeling of Physical and Data Link Layer Security Attacks in WSN"*, International Journal of Computer Applications, Volume 70– No.11, May 2013.

[2] Li, Hong, Y. Chen, and Z. He. "The Survey of RFID Attacks and Defenses." 8th International Conference on IEEE Wireless Communications, Networking and Mobile Computing (WiCOM), 2012.

[3] F. Kandah, Y. Singh, W. Zhang and C. Wang, "Mitigating colluding injected attack using monitoring verification in mobile ad-hoc networks", Security and Communication Networks, pp.1939-0122,2013.

[4] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 32-37. doi: 10.1109/I-SMAC.2017.8058363

[5] M.U. Farooq, M. Waseem, A. Khairi, S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", International Journal of Computer Applications (0975 8887), Volume 111 - No. 7, February 2015.

[6] I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), pp.180-187,Larnaca, 2015.

[7] Md. I. Abdullah,M. M. Rahman and M. C. Roy, "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count" I. J. Computer Network and Information Security, pp.50-56, 2015.

[8] Wahid, Abdul, P. Kumar, "A Survey on attacks, Challenges and Security Mechanism In wireless Sensor Network", JIRST- International Journal for Research in Science & Technology, Volume 1, Issue 8, pp. 189-196,January 2015.

[9] Zulkifli, M. Zaid W. Mohd, "Attack on Cryptography", (2008).

[10] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, vol. 78, pp. 544–546, Jan. 2018.

[11] S. K. Josyula and D. Gupta, "A new security methodology for internet of things," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, 2017, pp. 613-618.doi: 10.1109/CCAA.2017.8229874.

[12] C. Tian, X. Chen, D. Guo, J. Sun, L. Liu and J. Hong, "Analysis and design of security in Internet of things," 2015 8th International Conference on Biomedical Engineering and Informatics (BMEI), Shenyang, 2015, pp. 678-684.doi: 10.1109/BMEI.2015.7401589.

[13] Z. Yorio, R. Oram, S. El-Tawab, A. Salman, M. H. Heydari and B. B. Park, "Data analysis and information security of an Internet of Things (IoT) intelligent transit system," 2018 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, 2018, pp. 24-29. doi: 10.1109/SIEDS.2018.8374744.

[14] A. Yousefi and S. M. Jameii, "Improving the security of internet of things using encryption algorithms," 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, 2017, pp. 1-5.doi: 10.1109/ICIOTA.2017.8073627.

[15] J. K. Ahuluwalia and U. Khanna, "New technique for increasing security management using Internet of Things (IOT) application," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 1581-1584.doi:10.1109/ICPCSI.2017.8391977

[16] Yehia, L. , Khedr, A. and Darwish, "A. Hybrid Security Techniques for Internet of Things Healthcare Applications." Advances in Internet of Things, 5, 21-25. doi: 10.4236/ait.2015.53004.

[17] R. Hussain and I. Abdullah, "Review of Different Encryptionand Decryption Techniques Used for Security and Privacy of IoT in Different Applications," 2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, 2018, pp. 293-297. doi: 10.1109/SEGE.2018.8499430.

[18] Singh, Meena & m a, Rajan & V L, Shivraj & Purushothaman, Balamuralidhar. (2015). "Secure MQTT for Internet of Things (IoT)." 746-751. 10.1109/CSNT.2015.16.

[19] Z. Ren, X. Liu, R. Ye and T. Zhang, "Security and privacy on internet of things," 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), Macau, 2017, pp. 140-144. doi: 10.1109/ICEIEC.2017.8076530

[20] Liu X, Zhao M, Li S, Zhang F, Trappe W. A Security Framework for the Internet of Things in the Future Internet Architecture. Future Internet. 2017; 9(3):27.

[21] Jain, Pragya and Sardana, Anjali, "Defending against Internet Worms Using Honeyfarm", Proceedings of the CUBE International Information Technology Conference, pp.795-800,2012.

[22] Ammar, Mahmoud & Russello, Giovanni & Crispo, Bruno. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications. 38. 8-27. 10.1016/j.jisa.2017.11.002.