BKH1925006F

by Iftekhar Efat

Submission date: 13-Mar-2022 03:05AM (UTC-0400)
Submission ID: 1782995741
File name: BKH1925006F.pdf (178.57K)
Word count: 1395
Character count: 7950

Effective cybersecurity methods in the Internet of Things

Nadia Islam
BKH1925006F

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security ....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

In submitting this work I am indicating that I have read the University's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

I give permission for this work to be reproduced and submitted to other academic staff for educational purposes.

OPTIONAL: I give permission this work to be reproduced and provided to future students as an exemplar report.

Abstract

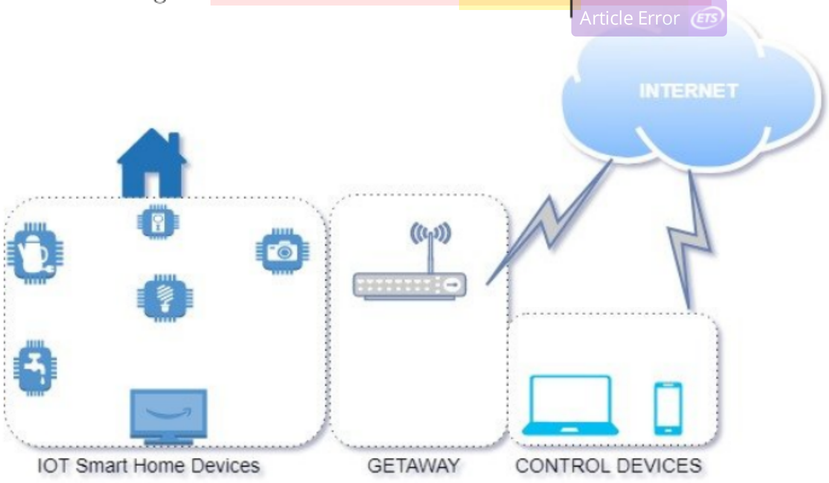
As an emerging technology, the Internet of Things (IoT) revolutionized the global network comprising of people, smart devices, intelligent objects, information, and data. The current IoT is facing increasingly security issues, such as vulnerabilities of IoT systems, malware detection, data security concerns, personal and public physical safety risk, privacy issues, data storage management following the exponential growth of IoT devices. This work aims at investigating the applicability of computational intelligence techniques in cybersecurity for IoT, including CI-enabled cybersecurity and privacy solutions, cyber defense technologies, intrusion detection techniques, and data security in IoT.

1 Introduction

Internet of things (IoT) refers to various electronic devices and objects that are able to connect, and transfer data through the seamlessly Internet. The adoption of IoT devices in the home environment has tremendously increased these years in order to fulfill the user needs and provide value and convenience to our daily activities [2].

In a smart home, IoT technologies are used to make the homes smarter in order to improve security, efficiency, and comfort. Hence, the smart home domain is considered as the main factor of the Internet future.More than 90 million people around the world will live in smart homes. However, privacy and security in IoT environments have been identified as the key barriers of the smart home and they require attention. In the cyber era, the popularity of emerging technologies has led to more attention to the issues concerned with the privacy and security of services. In addition, there is no well-established practice from governments to enforce IoT-industries to design IoT devices with high security and privacy standards . Furthermore, the complexity and heterogeneity that massively interconnected services and devices may increase the challenges of embedding IoT devices at homes. The heterogeneous of smart home devices have many constraints in the hardware design, including the processing unit, energy, and storage limitations which will complicate the implementation of traditional security solutions on the constraint IoT devices. Moreover, the home services and the sensitive information should be protected against any malicious attacks that exploit the vulnerabilities of traditional security and monitoring system [20]. Thus, the smart home environment needs superior security methods and daily monitoring, backup, and software updating.

Figure 1: An environment of IoT-based smart home



2 Background

In IoT environment, the IoT devices are typically limited with resources, in terms of computation, storage, memory, power etc.; hence, new technologies that can match the needs for resource-constrained devices in IoT are necessary. Considerable research efforts on cyberthreat intelligence have been conducted in the past few years and a number of sophisticated techniques have been developed that can perform cybersecurity anomaly detection.

In broadly, computational intelligence algorithms have been used in IoT security solutions, i.e., malware detection, cyberthreats identification, suspicious behavior monitor, intrusion detection, stopping cyberattackers, etc. The CI techniques can enable the IoT upgrade its cybersecurity capabilities and protect IoT applications and users.

In smart home, the CI enabled techniques also brings threats to cybersecurity: it is reported that the CI techniques are used to develop techniques for unlocking doors and transferring money using devices such as Alexia, Siri, and Google Assistant in smart home without the knowledge of the smart home users. It can image that the CI techniques, such as financial sectors, pricing algorithms, smart environments, can be used by attackers targeting on IoT applications.

The using of CI techniques, it is possible to provide deeper security and simplify the process for security analysis. However, the cybercriminals can also use CI techniques to develop new threats that might be more difficult to identify. In this case, the organizations need to well design the security strategies and use data-centric security models. However, cybercriminals are also using more intelligent tools to commit cybercrimes. It is possible that the CI are used to make IoT malware turn into a weapon. Dilek et al. reviewed the CI based techniques in cybercrime [10], including the vulnerabilities and threats identification in intrusion detection systems using the most recent CI techniques.

3 Classification of key management of Cyber Security

Before evaluating various key management schemes, we are going to explain some preliminary concepts of key management in cryptography. Symmetric key cryptography also known as shared key

ciphers/algorithms is that type of cryptography in which the same key is used by both the sender and receiver for the encryption and decryption of plaintext and ciphertext, respectively. Key management schemes are mainly classified into two broad classes, that is, static and dynamic[1].

3.1 Dynamic Key Management Schemes (DKM)

Different keys are assigned for various sessions in dynamic key management schemes. The keys for the next session will be dynamically issued to nodes without any revocation or updating instruction after the communication session between the sender and receiver has stopped or concluded. The keys are created dynamically in dynamic key management schemes because communication is supposed to be initiated between the sender and receiver in three main fashions:

1. contributory
2. centralized
3. distributive

Various keys are allocated for different sessions in dynamic key management schemes, on the other hand. When the sender and receiver's communication session ends, the key for the next session is generated[1].

3.2 Static Key Management Schemes (SKM)

In static key management methods, the key is produced by mutual agreement, symmetric cryptography, or centralized certifying authority, asymmetric cryptography, for the whole lifespan of the nodes. Keys are allocated to nodes throughout the lifetime of the node in the static key management technique, whereas keys are assigned to nodes for each session in the dynamic key management approach. The key is produced in static key management systems either by mutual agreement, as in symmetric cryptography, or by a certifying authority, as in asymmetric cryptography[1].

4 Evaluation

In this study, we investigated and compared several schemes in terms of the services provided and threats avoided in MANETs, WSNs, and the Internet of Things. In addition, the disadvantages and limits of the suggested systems are evaluated in terms of vulnerabilities and assaults that are not addressed. Table 1 summarizes the various security services discussed here. Intruders cannot access confidential information. Intruders can't read integrity since it's unreadable. Authentication refers to a system that is only available to authorized users. Nonrepudiation occurs when one or both of the sender and recipient deny later after the data has been sent. Availability refers to ensuring that the service is available at all times, 24 hours a day, seven days a week. Attacks can be either active or passive, depending on how they affect the data.

Eavesdropping, sniffing, wiretapping, and other passive attacks are examples. All of these attacks have the potential to disrupt the confidentiality service ,while active assaults allow the intruder to alter or destroy the data's contents or source. Modification, insertion, impersonation, repudiation, and denial of service assaults are examples of active attacks. All of these attacks can be used to disrupt services that provide integrity, authentication, nonrepudiation, and availability

References

[1] Mohammad Faisal, Ikram Ali, Muhammad Sajjad Khan, Junsu Kim, and Su Min Kim. Cyber security and key management issues for internet of things: Techniques, requirements, and challenges. *Complexity*, 2020, 2020.

[2] In Lee. Internet of things (iot) cybersecurity: Literature review and iot cyber risk management. *Future Internet*, 12(9):157, 2020.

BKH1925006F

ORIGINALITY REPORT

75%	73%	45%	38%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	paper.ijcsns.org Internet Source	20%
2	www.hindawi.com Internet Source	17%
3	uwe-repository.worktribe.com Internet Source	16%
4	v1.overleaf.com Internet Source	6%
5	Shanshan Zhao, Shancang Li, Lianyong Qi, Li Da Xu. "Computational Intelligence Enabled Cybersecurity for the Internet of Things", IEEE Transactions on Emerging Topics in Computational Intelligence, 2020 Publication	5%
6	ieeexplore.ieee.org Internet Source	5%
7	Submitted to Colorado Technical University Online Student Paper	2%

8	Mohammad Faisal, Ikram Ali, Muhammad Sajjad Khan, Junsu Kim, Su Min Kim. "Cyber Security and Key Management Issues for Internet of Things: Techniques, Requirements, and Challenges", Complexity, 2020 Publication	1 %
9	global.oup.com Internet Source	1 %
10	www.coursehero.com Internet Source	1 %
11	www.towncountryservices.com Internet Source	1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

BKH1925006F

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

PAGE 3

PAGE 4

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

PAGE 5

Article Error You may need to use an article before this word.

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Sentence Cap. Remember to capitalize the first word of each sentence.

PAGE 6

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 7

Article Error You may need to use an article before this word.

PAGE 8

Missing "," You may need to place a comma after this word.