Chapter 7
A Review on Cyberattacks: Security Threats and Solution Techniques for Different Applications

Gaganjot Kaur Saini
Charles Sturt University, Australia

Malka N. Halgamuge
https://orcid.org/0000-0001-9994-3778
Charles Sturt University, Australia

Pallavi Sharma
Charles Sturt University, Australia

James Stephen Purkis
Charles Sturt University, Australia

ABSTRACT

Research questions remain to be answered in terms of discovering how security could be provided for different resources, such as data, devices, and networks. Most organizations compromise their security measures due to high budgets despite its primary importance in today's highly dependent cyber world and as such there are always some loopholes in security systems, which cybercriminals take advantage of. In this chapter, the authors have completed an analysis of data obtained from 31 peer-reviewed scientific research studies (2009-2017) describing cybersecurity issues and solutions. The results demonstrated that the majority of applications in this area are from the government and the public sector (17%) whereas transportation and other areas have a minor percentage (6%). This study determined that the government sector is the main application area in cybersecurity and is more susceptible to cyber-attacks whereas the wireless sensor network and healthcare areas are less exposed to attack.

DOI: 10.4018/978-1-7998-2466-4.ch007

INTRODUCTION

The term "Cyber Security" refers to protecting all networks, computing/smart devices and data/information from vulnerabilities and hackers. This is needed because all security techniques, including firewalls and anti-virus measures, are still vulnerable in terms of protecting cyber security systems from attacker (Kumar, Yadav, Sharma, & Singh, 2016). Attackers can be categorized as intentional (attackers who have some kind of personal motive and benefit by hacking or attacking devices and networks) or non-intentional (attacker that may mistakenly or unknowingly send some kind of malicious code to the devices or network). There are three categories of attacks; (i) Network attacks (Intrusions, Web defacement, Denial-of-Service attacks), (ii) Network abuse (Phishing, Forgery, SPAM) and (iii) Malicious codes (Viruses, Worms, Trojen horse, Spyware, Key loggers, BOTs). Cyber threats can take the form of cyber war, cyber terrorism and cyber-crime. Firstly, cyber war occurs when one country aims to destroy the networks and computing devices of another nation, for example Denial of Service attacks and viruses (Kumar et al., 2016). Secondly, cyber terrorism occurs when terrorist organizations or groups organize activities using cyber means that cause or spread terror, for example network attacks and hacking systems (Kumar et al., 2016). Lastly, cyber-crime is motivated by data theft, monetary gain or wicked- hacking, for example, Debit/credit card data, crashing website (Kumar et al., 2016).

Cyber security is very crucial when it comes to protecting devices, data and networks in this field. This field includes banking, finance, insurance, education, telecommunication, taxation, and accounting. Moreover, privacy and security remain significant areas of study because there are always different types of issues in protecting data, networks and devices. In terms of security, it is important to consider what, who and how is involved. That is, what devices to protect, who is authorized to apply these measures and how the devices should be protected. Importantly, every sector depends on Information Technology and the internet for doing its operations (P. Chauhan, N. Singh, & N. Chandra, 2013). Consequently, privacy and security are important topics, which every company needs to be concerned about. Almost everything in our daily life is connected to technology such as of communication, transportation and health care (P. Chauhan, N. Singh, & N. Chandra, 2013). Moreover, human beings are completely dependent on technology such as people using phones and computers for communication as well as the internet for online shopping and e-billing. Hence, attackers have more options to hack these systems than ever before. Furthermore, this dependence on technology and the internet has led to more potential vulnerabilities for attackers to exploit (H. Iguer, Medromi, Sayouti, Elhasnaoui, & Faris, 2014). Cyber security in transportation systems is also very crucial otherwise attackers can take advantages of the in-vehicle or other vulnerabilities in GPS, security cameras, emergency communication (two-way radios) and other related systems (Bowen et al., 2015).

Smart City is a new concept and there is no proper definition yet. However, a smart city can be described as a city, which includes ICT for improving the superiority as well as execution of metropolitan services, e.g. transportation, electricity and other conveniences for diminishing wastage, and overall cost consumption of resources ("Smart City,"). The main objective of the smart city is to improve the quality and life style of the citizens by using smart technology ("Smart City,"). A smart city includes all the facilities for its citizens such as proper supply of water, electricity, sanitation, management of wastes, transportation services, security and safety, education, health services, sustainable environment, housing and other digital services for making life easier than ever before ("Features of Smart Cities,").

Different authors have proposed different solutions for different issues in cyber security. Some suggest preventative measures while others seek to identify attacks. For instance, there are the following