International Journal of Communication and Information Technology

E-ISSN: 2707-6628
P-ISSN: 2707-661X
IJCIT 2020; 1(1): 51-54
Received: 15-11-2019
Accepted: 21-12-2019

Pratishtha Bowade
Department of Information Technology Sagar Institute of Research & Technology Bhopal, India

Jay Kumar Jain
Department of Information Technology Sagar Institute of Research & Technology Bhopal, India

Rakesh Kumar
Department of Information Technology Sagar Institute of Research & Technology Bhopal, India

Corresponding Author:
Pratishtha Bowade
Department of Information Technology Sagar Institute of Research & Technology Bhopal, India

A detailed survey on cyber security and its challenges

Pratishtha Bowade, Jay Kumar Jain and Rakesh Kumar

DOI: https://doi.org/10.33545/2707661X.2020.v1.i1a.9

Abstract
Cyber security is a way of protecting our useful information, entire network, and the system from different attacks to avoid damage. The cyber security threat is peculiar towards the Government, Military, Corporate, Financial and Medical organizations because they collect, process, and store unprecedented amounts of data on computers and other devices. In this research paper researcher discuss about the technologies and challenges towards the Cyber Security. Researcher also discusses about the benefits of Cyber security.

Keywords: Cyber Security, Network, Technology, Threat.

Introduction

Cybercrime is a global problem that has dominated the news cycle. It poses a serious threat to the safety of individuals and to the greatest threat to large multinational companies, banks and governments. Today's organized cybercrimes are high level hackers of the past now that large scale organized art works as a starting point and they often hire professionals who are trained to do regular online attacks. With so many cyber security data out there, cyber security has become crucial. Cyber security is important because it includes everything related to protecting our sensitive data, sensitive information, Protected Health Information (PHI), personal information, intellectual property information, and government and industry information systems for theft and damage to criminals and enemies. An important part is that data have sensitive information, regarding intellectual property, financial data, personal information, or other types of data where unauthorized access or disclosure could have the serious consequences. Cyber security is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and other important data from malicious attacks. Cyber security is also known as information security or electronic data security. A cyber security strategy focuses on prevention, detection, response and recovery. This whole strategy can be applied to other security strategies that require the definition and implementation of the Smart Grid cyber security risk assessment process. Risk is an unwanted result that is triggered by an event, event, or event, as determined by its usefulness and its associated impacts. This type of risk is one risk factor for an organization, which can include many types of risk (e.g. investment risk, budget risk, program management risk, legal liability risk, security risk, inventory risk, and risk from information systems) [4, 5, 7]. The Smart Grid risk assessment process is based on the risk assessments already carried out by both the private and public sectors and includes identifying assets, risks and threats and specifying the impacts to produce a risk assessment for Smart Grid and its domains and sub-sites, such as homes and businesses. Because Smart Grid incorporates systems from IT, telecommunications and electrical systems, the risk assessment process is applied across all three sectors as it integrates with Smart Grid. The information included in this report is a directory of organizations. NIST does not specify specific solutions for the directory contained in this report. Each organization should develop its own detailed cyber security methodology (including a risk assessment method) for Smart Grid [8, 10, 11]. The following security terms which have been used normally in the field of computer security?

Unauthorized access: Unauthorized access is when a person obtains access to a server, website, or other sensitive information using another person's account information.

Hacker: Is a person who tries and uses a computer program for financial, social reasons, fun etc.

Threat: An event that may compromise safety.

Damage: It is a weakness, design problem or implementation error that can result in an unexpected and unpleasant event regarding a security program.

Attack: It is a system security attack brought by a person or machine to the system. It is a breach of security.

Antimalware: Is software that runs on a different OS used to protect malicious software?

Virus: It is malicious software that infects your computer without your permission for bad purpose.

Firewall: It is software or hardware used to filter network traffic based on rule

A. Inside Cybercrime
Cybercrime is a serious issue for the cyber society. The major types of cybercrime are:

B. Hacking
It is an illegal practice where a hacker violates someone's computer security program for their purpose.

C. Unnecessary sharp focus
Large employment means the surveillance of a large part of a group of people by the authorities especially for security purposes, but if a person does it for their own good, it is considered to be cybercrime.

D. Child pornography
It is one of the most horrific crimes in the world. Children are sexually abused and videos are made and uploaded to the Internet.

E. Child grooming
It is the practice of establishing emotional contact with a child especially for the purpose of trafficking children and child prostitution.

F. Copyright infringement
If a person infringes a copyright protected without permission and distributes that in their own name, this is known as copyright infringement.

G. Money laundering
Illegal detection by an individual or organization is known as money laundering. It usually involves the transfer of funds by foreign banks and / or legal entity. In other words, it is the practice of converting illicit money into a formal financial system.

H. Cyber hacking
When a shooter hides someone else's email server, or computer program and demands money to re-install the system, it's known as cyber hacking.

I. Cyber terrorism
Usually, when a person files a government security plan or intimidates a government or a large organization to advance their political or social goals by attacking the security system through computer networks, it is known as cyber terrorism.

2. Literature Review
Vidhya P.M in his research paper “Cyber Security - Trends and Challenges” discuss about the cyber security field trends, challenges and cyber ethics [1]. Jang-Jaccard and S. Nepal in their research paper "A survey of emerging threats in cyber security” describe about the new attack in emerging technologies which are helpful in the current scenario [2].

W. Bradley Glisson and K. Kwang Raymond Choo, in their research paper “Introduction to the Minitrack on Cyber-of-Things: Cyber Crimes, Cyber Security and Cyber Forensics discuss about the novel solutions which is supportive in cyber forensic investigations in cyber-of-things at large context [3].

Adel. e. M. Elsawy in his research article “E-Learning using the Blackboard system in Light of the Quality of Education and Cyber security” describe about the importance of linking e-learning with cyber security [8].

3. Towards cyber security
There is safe learning and provides an excellent opportunity to provide education opportunities to many community groups. Working to protect and secure data and information circulating through e-learning networks is very effective. The statement of the value of e-learning through the Blackboard program lies in providing time and effort for the student and the professor and provides for the costs of the University, and is an effective way of learning. The use of electronic learning works to increase student learning success compared to the traditional approach. The importance of shared classroom buildings as one of the major ways to provide online courses and lectures online as they transcend temporal and spatial and functional training in distance learning and help to spread education and practice the student can read well. E-learning is coupled with modern educational technology in the process of transferring information and reliance on printed media, magazines, magazines, and research, which further promotes the possibility of expanding this form of education and spreading its benefits to all members of the public Recommendations [4, 6, 8].

Currently an online system, such as hardware, software and data can be secured to cyber attacks through cyber security. Cyber security is a set of technologies and processes designed to protect computers, networks, systems and data from attacks and unauthorized access, modification, or destruction. As threats become more sophisticated such technologies as machine learning (ML) and deep learning (DL) are being used in the cyber security community to enhance security capabilities. Nowadays, cyber security is a renewed issue in the cyber space and has always been supported on computer of different application domains such as finance, industry, medical and many other important areas. The identification of various network attacks, especially those that have never been seen before, is a major problem to be resolved urgently. This paper discusses the previous work of machine learning (ML) and deep learning methods (DL) for cyber security applications and the specific application of each method in cyber security operations. The ML and DL methods covered in this paper are effective in detecting cyber security threats such as hackers and hackers, spyware, phishing and ML / DL internet access. Therefore, the main prominence is placed on the accurate description of the ML / DL methods, and

references to the signal function of each ML and DL method. Also discuss the challenges and opportunities of using ML / DL to get cyber security [5, 7, 9].

4. Benefits of cyber security

A. Protection of business

The big advantage is that IT security IT security solutions can offer your business completely. This will allow your employees to use the internet when and where they need to, and to make sure they are not vulnerable from potential threats.

B. Protection of Personal Information

One of the most important assets in the digital age is personal information. If the virus has access to personal information about employees or customers, is able to sell that information, or use it to steal their money.

C. Provide Protection to employee for their work

Without the best cyber security solutions for your business, you and your employees are always at risk of cyber attacks. If your system, or any other computer, is infected with this virus it can damage its product and force you to switch computers.

D. Protect Productivity

Viruses can slow your computers to light, and make working on them difficult. This can create a huge waste of time for your employees, and often bring the rest of your business to a halt.

E. Provide Safety to your Website

As a business, chances are you are in charge of your website. If your system becomes infected, there is a very good chance that your website will be forced to shut down. This means that you will not only lose money from missed payments, but will also lose customer trust and certain viruses that can permanently damage the system.

F. Denial Spyware

Spyware is a cyber infection designed to spy on your computer's actions, and then transmits that information back to cyber-criminals. A great cyber security solution, such as Fortinet's Fort iGATE firewall, can prevent this spyware from being activated and ensure that your employees' actions remain private and confidential within your work environment.

G. Prevention of Adware

Adware is a computer virus that fills your computer with ads and is normal. However, all of these ads can impact productivity and will often allow other viruses to enter your computer as long as you click on them accidentally.

H. Integrated solution

The best IT security features for your business will provide a comprehensive security solution against various problems. Ideally, your security needs to include firewall, anti-virus, anti-spam, wireless security and content filtering online. Find out how your business can benefit from a Fabric-based security system.

I. Support Your IT Expert

It may be good to hear, but most cyber criminals will have more information than your average employee when it comes to digital crime. The best IT security systems can provide your team with the features and support they need to successfully fight a high risk criminal.

J. Encourage Confidence in Your Clients

If you can prove that your business is successfully protected from all kinds of cyber threats, you can encourage trust in your customers and your customers. They will feel more confident when purchasing your products or using your services.

5. Challenges in cyber security

An important challenge for cyber hacking is the lack of qualified service professionals. There are many people on the lower end of the cyber security spectrum with generic skills. Security experts do not know how to protect companies from the most vulnerable hackers. Those who can do things understand how they want things. When they work, they charge money that very small businesses cannot afford. Only the largest and richest companies in the world can afford these high-quality services, another obstacle that SMBs have to overcome is online competition [1, 3, 5].

With various income groups in India, not everyone can afford expensive phones. In the US, Apple has a market share of over 44%. However, in India iPhones with their high security standards are used by less than 1% of mobile users. The growing gap between the security afforded by the high end iPhone and the low cost of advertising makes it almost impossible for legal and technical standards to be set for data protection by regulators [2, 6, 8].

Machine to Machine Technology which is the subset of internet of things helps physical devices can be accessed through the Internet. Physical devices connected to each other and have a unique identification number and these devices able to transfer data or information to a network without any need of communication to human. The firmware and software running on IoT devices make consumers and businesses more susceptible to cyber attacks [7, 8, 10, 11].

6. Conclusion

This paper provides an overview of the most important aspect of security in the world of economic distribution and information. The role of social media, cyber security and cyber terrorism has been described. With the increase of Internet users is directly proportional to an increase in cyber crime along with hacking. The researcher concluded that the person who uses internet for their working should aware about the cyber crime. The researchers concluded

that individual should aware to recognize online security staple such as changing passwords regularly, keeping long passwords, to avoid disclosure personal information to strangers on the internet or installing credit card information on unsecured websites to avoid them any fraud.. The government is making efforts to control these acts of cyber crime. The government has it develop cyber laws to help people be educated about cyber crime. Another major threat of the technological war is that no one can predict time again Source of distinguished work. It can be set up remotely, and often is a multiplication of infringement is only available after serious damage. The researcher also concluded the effect of cyber security in different technologies like E-learning, Deep learning and Machine learning. Researcher concluded that hackers can use AI and

Machine Learning to design new solutions to create more sophisticated attacks. Researcher concluded that it is not possible to eliminate cyber crime from cyber space but it is possible to look at them. History proves that no law is effective in completely eradicating global crime and the only possible step is to make people aware of rights and duties.

7. References

1. Vidhya PM. Cyber security-Trends and Challenges. International Journal of Computer Science and Mobile Computing. 2014; 3(2):586-590.
2. J Jang-Jaccard, S Nepal. A survey of emerging threats in cyber security," Journal of Computer and System Sciences. 2014; 80:973-993.
3. W Bradley Glisson, KKwang Raymond Choo Introduction to the Minitrack on Cyber-of-Things: Cyber Crimes, Cyber Security and Cyber Forensics," In Proc. Hawaii International Conference on System Sciences, 2018, 5574-5575.
4. G. Nikhita Reddy and GJ Ugander Reddy. "A STUDY of cyber security challenges and its emergning trends on latest technologies," arXiv, 2014.
5. Y XIN. "Machine Learning and Deep Learning Methods for Cybersecurity"' IEEE Access. 2018; 6: 35365-35381.
6. H Li, J Masters. "E-Learning and knowledge management in the early years: Where are we and where should we go, Knowledge Management and eLearning," Knowledge Management & E-Learning: An International Journal. 2009; 1(4):245-250.
7. MM Chaturvedi, MP Gupta, Jaijit Bhattacharya. "Cyber Security Infrastructure in India: A Study," Emerging Technologies in E-Government, 2014, 70-84.
8. A e M.Elsawy. "E-Learning using the Blackboard system in Light of the Quality of Education and Cyber security," International Journal of Current Engineering and Technology. 2019; 9(1):49-54.
9. S Karbhari, R Gunjan. A survey of cyber security operations based on Machine learning & Deep learning"' Universal review. 2019; 8(2):168-173.
10. W Wanga, Z Lua. Cyber Security in the Smart Grid: Survey and Challenges," Elsevier, 2012, 1-29.
11. Hawk C, Kaushiva A. "Cyber security and the Smarter Grid" The Electricity Journal. 2014; 27(8):84-95.