International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 09 | Sep 2021 www.irjet.net p-ISSN: 2395-0072

CYBER SECURITY

HARSHA N MURTHY[1], NANDAN R[2]

ABSTRACT: Cyber Security plays a crucial role within the field of information technology. Preventing data theft has become one of the largest challenges lately. The primary issue that involves cyber security is cybercrimes which have seen a sharp increase over the past decade and continue to grow in number to date. Numerous governments and corporations are taking several measures to stop these cybercrimes. This paper primarily focuses on cyber security and the newest technologies to combat cybercrimes. It additionally focuses on the latest regarding the cyber security techniques, ethics and also the dynamic changes facing cyber security.

INTRODUCTION

Computer Science has been defined differently by various academicians and learning institutions. It entails the study of computer software and networks and how they function. The theoretical, designing and execution aspects of these digital systems are also studied under computer science. Additionally, the calculations and computability elements of the digital networks are entailed in the study subject. Mastery of these aspects of the subject helps solve complex algorithms, implement codes via different programming languages, and deal with different data structures, among others. All these components are studied under the different sub-topics of the field. Some of the topics include the study of algorithms, calculation complexity, linguistic designs, programming techniques, artificial intelligence, data reclamation, and cybersecurity. This paper will focus on the importance of cyber security in the new era of digitalization. This is because of the fact that Cyber-Security is more important than ever before. It allows people to use information technology to benefit our lives in many ways. However, the internet also has certain drawbacks which if not taken care of can lead to catastrophes. People have become so dependent on the internet that they are not able to live moments without using it. A new generation has grown up with very limited capabilities of functioning without technology and this is where cyber security comes in. It is the new generation of digitalization and it is the future.

Cyber Security can be defined as a procedure to carry out in order to protect computer networks, devices, information, and services from any kind of cyber-crime or any other cyber-attacks. This procedure includes things like network firewalls to antivirus software's. Anything that will keep you safe from malicious actions online basically can be named as Cyber Security. It controls the whole process to make sure users are not subjected to any malicious attacks or traitors. Moreover, it has recently become a lot important because people are becoming so reliant on technology that without it they are unable to function properly.

Cyber security is a specialised area of computer science which deals with protecting information and computer systems from unlawful intrusions and damaging effects caused by attacks, tampering, theft, and hacking. The system security targets protecting data from theft, malicious attacks, sabotage, spoofing, disclosure of data without permission or beyond the authorized accesses. It is also proposed to mitigate illicit use of facilities through its encryption mechanisms. Cybersecurity is also termed information technology (IT) security. This practice entails the defence of digital networks such as computers, network servers, information, and mobile gadgets from any form of malicious acts. The best methods to avert cyber-attacks are to implement preventive measures, stop criminal activities before they happen, and reverse the damage caused by the illicit acts. Security researchers often state that security breaches are inevitable in information-based systems, but can be mitigated through implementing robust security controls.

METHODOLOGY

Security depends on the effectiveness of the protection strategies employed against threats. These strategies help control accesses, manage change requests, manage data, protect user identities and privileges, limit access to sensitive data or resources by specific users or groups of users. Additionally, it helps in verifying the accuracy of transaction records in transactional systems. These malicious acts are usually aimed at having illegal access to individual's personal information, illicit obtaining of finances from individuals, tampering with sensitive data, or interfering with normal commercial transactions. The acts are performed by individuals with criminal intentions of stealing money, passwords, and other information they may have particular interests in. Under cyber-security, there are different categories of practice. Some of them include network security, data security, disaster recovery, and functional security. Each of these listed subcategories gives a specific focus on different elements of digital operations.

Network security deals with the safeguarding of digital networks from illegal access. This illicit intrusion could be from individuals attempting to intrude or harmful malware. Data security ensures all the sensitive information is protected and its integrity is maintained. This safeguarding is guaranteed in both storage and transfer of the data. On the other hand, disaster recovery describes the means of institutional response to digital attacks or harmful practices that result in information loss. This subcategory also includes governing regulations which describe how the corporate house reclaims its normal functioning and data lost to its previous state before the incidents. Lastly, the functional security sub-division deals with full protection of all the practices, processes, and relevant selections involved in handling the institution's informational resources. These are among the few components listed under information technology security.

Most business minds have termed cyber security as a critical component for the successful execution of any business undertaking. The main reason is that these days, most businesses are digital-based. And the digital medium is highly vulnerable to attacks. As a result, this has increased their need to protect their data from illegal access by malicious third parties. This has caused developers to deploy various data security measures to prevent hackers from gaining illegal access to a company's information or services. These actions are also meant to ensure that its clients' sensitive data remains confidential at all times.

The ever-increasing use of the internet and its cutthroat competition have resulted in having huge amounts of data either lost or corrupted on daily basis. Cybersecurity is essential in dealing with data-related processes and assets due to various reasons. First, it ensures all the company data is not given out to irrelevant third parties who could use it for their gains leading to incurring losses within the institution. The theft and tampering of organizational information could result in stagnation and decline company productivity and performance (Kweon et al., 2019). Another important justification for cybersecurity study is that it prevents upcoming markets from risks such as information tampering and damages. Currently, there are a lot of emerging commercial markets online. To protect them from any possible digital attacks, they should employ cyber-security techniques in trading processes. Sovereign state governments also need to secure data for their country as they store very sensitive information for their populations. Therefore, given a chance to further continue with my master's degree in computer science, I would specialize in cyber-security to make the digital world a safer place.

CONCLUSION

Today due to high internet penetration, cybersecurity is one of the biggest need of the world as cybersecurity threats are very dangerous to the country's security. Not only the government but also the citizens should spread awareness among the people to always update your system and network security settings and to the use proper anti-virus so that your system and network security settings stay virus and malware-free.

REFERENCES

1. Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks, and cybersecurity. Procedia Computer Science, 149, 65-70. https://doi.org/10.1016/j.procs.2019.01.108
2. Husak, M., Komarkova, J., Bou-Harb, E., & Celeda, P. (2019). Survey of attack projection, prediction, and forecasting in cybersecurity. IEEE Communications Surveys & Tutorials, 21(1), 640-660. https://doi.org/10.1109/comst.2018.2871866
3. Kweon, E., Lee, H., Chai, S., & Yoo, K. (2019). The utility of information security training and education on cybersecurity incidents: An empirical evidence. Information Systems Frontiers. https://doi.org/10.1007/s10796-019-09977-z
4. Salatino, A. A., Thanapalasingam, T., Mannocci, A., Osborne, F., & Motta, E. (2018). The computer science ontology: A large-scale taxonomy of research areas. Lecture Notes in Computer Science, 187-205. https://doi.org/10.1007/978-3-030-00668-6_12