Cybersecurity Threat Detection & Protection System

Bangladesh University of Business & Technology

Team Member:

Tanvir Hossain Khan (18192103203)

Rifatul Islam (18192103187)

Al Shahriar Emon (18192103229)

Hassan Al Mahmud (18192103239)

MD Hasibur Rahman Redoy (18192103276)

Supervised By:

Mr.M.M. Fazle Rabbi

Assistant Professors

Department Of CSE, BUBT

Table of Contents **Page Number.**

Abstract

Cybersecurity is one of the main study issues of the current digital era due to the expanding internet services. Cybersecurity is the practice of preventing unauthorized access to systems, hardware, software, networks, and electronic data. To identify various sorts of attacks, a cyber-security system must be constructed. The use of various intelligence algorithms in cybersecurity enabled the detection and analysis of attacks on computer networks. Artificial intelligence, machine learning, and deep learning algorithms are used in cybersecurity to take the best feature representation out of a large data set. This has been used in several cybersecurity scenarios, including the analysis, prediction, and detection of attacks. The purpose of this work is to analyze cybersecurity attack datasets using clever methods.

Additionally, it offers a detailed comparison of algorithm performance and field application to explain the advantages of network protection optimization methods.

Introduction:

With the increasingly in-depth integration of the Internet and social life, the Internet is changing how people learn and work, but it also exposes us to increasingly serious security threats. How to identify various network attacks, particularly not previously seen attacks, is a key issue to be solved urgently. With the development and advancement of information technology, humans have become extremely efficient in work, study, and communication, but at the same time, people's definition of privacy and security is constantly being refreshed. Cyber security is the set of applying security preventions to provide confidentiality, integrity, and availability of data. Cyber security is a significant research area because all of the operations based on government, military, commercial, financial and civilians gather, process, and store tremendous volume of data on computers and others. Cyber security is not just a problem of IT field. In fact, its scope is very vast. Today everyone is familiar with internet. Even illiterate people are using smart phones and it has become indispensable from their day-to-day life. Without proper knowledge and awareness, everyone is using AI in their daily walks of life. This is the golden opportunity for hackers to deceive the people easily. At times, hackers are also cheating the people who are having sound knowledge on AI. There for cyber security is a mutual problem across the globe. Hackers are becoming smarter day by day and they are more innovative in creating malicious software to exploit the vulnerable data of individuals, organizations and governments. It attacks are increasing rapidly despite of enough security measures. Cyber can be in the form of malicious software, phishing, password attacks, drive by downloads by using hyperlinks, virus attacks etc.

Literature Review

[1] The paper discuss about the use of artificial intelligence (AI) to improve information security. Aside from working to develop detached defensive lines, a need to recognize utilizing active security systems. Data were gathered from academic and industrial sources. The research found that the use of AI in cyber warfare direct authority has both benefits and disadvantages. This detection approach is likely to boost business and customer security in the cyber world.

[2] This paper discuss about effectiveness of artificial intelligence techniques against cyber security risks. The aim of the researcher was to determine the effectiveness of artificial intelligence techniques. The overall results of the study indicated that AI has become one of the primary assets for firms to improve their performance in terms of cyber security.The findings of the study revealed that all independent variables had significant and positive relation apart from expert system.

[3] The paper discus about the survey of evolution of cyber security. If we look back we can see so many problem that it can't handle. For this so many complex data can be threated. The previously used conventional security systems are no longer sufficient because those systemterms lack efficiency in detecting previously unseen and polymorphic attacks. But when the machine learning came to meet cyber security the protection rate of cyber security protection has been increased. As a result so many polymorphic attack can be easily protected.

[4] The paper discuss about artificial intelligence in cyber-defense technologies. One of the most important things in the world, today is privacy. People need to worry more about invasion of their private life. With the advancement of technologies to provide us more comfort in our lives, even the bad side of it has surfaced more. Hackers use more complex algorithms to crack a network and steal very sensitive and confidential data, which might affect a single person or sometimes as large as a country.The number of cybercrimes are increasing very rapidly.

[5] The paper introduced about the power grid cyber security system. This paper is a state-of-the-art survey of cyber security R&D for a smart grid. The integration of computing and communication capabilities with the power grid has led to numerous vulnerabilities in the cyber-physical system. This cyber security threat can significantly impact the physical infrastructure, economy, and society.

Problem statement

Threat detection is the practice of analyzing the entirety of a security ecosystem to identify any malicious activity that could compromise the network. If a threat is detected, then mitigation efforts must be enacted to properly neutralize the threat before it can exploit any present vulnerabilities.

Getting breached is a nightmare scenario, and most organizations that prioritize their information will put smart people and technologies to work as a defensive barrier against anyone who might try to cause trouble. But security is an ongoing process—not a guarantee.

Within the context of an organization's security program, the concept of "threat detection" is multifaceted. Even the best security programs must plan for worst-case scenarios, when someone or something has slipped past their defensive and preventative technologies and becomes a threat.

Methodology

The main goal of the proposed deep learning methodology is to catch the pirated software from different types of source codes. A deep learning methodology is designed to detect plagiarism in various types of source codes. The plagiarized version of the software is the pirated copy in which cracker used the logic of the original software. First, the source codes are tokenized in preprocessing steps to reduce the dimensions of the data and extract meaningful features for next step.

Conclusion

This paper presented a decision Support System in form of a labeling system for cyber threats, that evaluates their severity regarding frequency of appearances/references and number of incidents. And lists of the involved cybercrime stakeholders, general preventive measures in form of good practices and customized ones depending on the characteristics of cybersecurity incidents.

Reference:

[1] Sun, C.C., Hahn, A. and Liu, C.C., 2018. Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, pp.45-56.

[2] Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *computers & security*, *38*, pp.97-102.

[3] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A. and Xu, M., 2020. A survey on machine learning techniques for cyber security in the last decade. *IEEE Access*, *8*, pp.222310-222354.

[4] C. R. Srinivasan, B. Rajesh, P. Sai Kalyan, K. Presager and E. S. Yadav, "A review on the different types of Internets of Things (IoT)", *J. Adv. Res. Dyn. Control Syst.*, vol. 11, pp. 154-158, 2019.

[5] Noam Ben-Asher, Alessandro Oltramari, Robert F Breacher, and Cleotilde Gonzalez. Ontology-based adaptive systems of cyber defense. In STIDS, 2015

[6] Gartner. Reviews for Security Information and Event Management (SIEM) Software. https://www.gartner.com/reviews/market/securityinformation-event-management. [Online; accessed 3-March-2018].

[7] Alex Vovk. How to Overcome SIEM Limitations. https://blog.netwrix. com/2016/03/21/how-to-overcome-siem-limitations/, 2016. [Online; accessed 2-March-2018].

[8] Alex Vovk. Infographics: Common Drawbacks of SIEM Solutions. https://blog.netwrix.com/2016/03/15/infographics-common-\ -drawbacks-of-siem-solutions/, 2016. [Online; accessed 2-March-2018].

[9] John R. Goodall. STUCCO: A cyber intelligence platform. https://www. ornl.gov/division/projects/stucco, 2017. [Online].

[10]