Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 13, No. 1, (2022),
ISSN : **1906-9685**

Journal of Nonlinear Analysis and Optimization : Theory & Applications

Editors-in-Chief :
Sompong Dhompongsa
Somyot Plubtieng

A Detailed Review on Cyber Security

Prachi Sharma

Assistant Professor

Computer Science Engineering

Arya Institute of Engineering & Technology, Jaipur

Pramod Kumar

Associate Professor

Dept. of IT

Arya Institute of Engineering & Technology, Jaipur

Payal Rathore

Science Student

Sant Meera Convent Senior Secondary School Pratapgarh, Rajasthan

Nilesh Kumar

Science Student

Kendriya Vidyalaya Masjid Moth, Sadiq Nagar , New Delhi

http://doi.org/10.36893/JNAO.2022.V13I02.0012-020

Abstract

Cyber security is critical in protecting people who use the internet through various electronic devices in their daily lives. Some causes have occurred worldwide, causing people to experience issues when connecting their devices and systems to the internet. Hackers pose a significant threat to extremely sensitive data such as biotechnology and military assets; cyber security plays a critical role in securing such data. Misuse of the internet has become a current issue in many areas of life, particularly in social media, universities, and government organizations. The Internet is extremely beneficial to students in educational institutions and employees in various organizations. People can obtain information from the internet by using an internet source. They must, however, be protected when using the internet and secure against unauthorized access. In this paper, we discussed various aspects of network security and cyber security in the modern era. We also attempted to cover threats in organizational intranets.

Keywords

Cyber Security, Cyber Crime, Cyber Attack, Countermeasures, A.I., ML

I. Introduction

Cybersecurity is a critical aspect of our digital world, and as college students, we must understand the following:- Cyber Security is a critical field in today's digital age, as it encompasses the protection of information systems, data from unauthorized access, and networks, damage, and theft. With the increasing reliance on technology in all aspects of our lives, the need for skilled professionals in this field has become more pressing than ever before. As a college student, understanding the importance of cybersecurity can open up a world of opportunities and contribute to a safer and more secure digital environment.

In today's interconnected world, cyber threats are constantly evolving and becoming more sophisticated. Therefore, it is crucial to stay ahead of these threats by developing strong technical skills and knowledge in areas such as network security, encryption, malware detection, and incident response. Pursuing a degree in Cyber Security can provide you with a solid foundation in these areas, equipping you with the necessary skills to protect valuable information and prevent cyber-attacks.

Furthermore, the demand for cybersecurity professionals is on the rise, with companies across all industries recognizing the potential risks associated with data breaches and cyber-attacks. As a college student, studying cybersecurity can lead to numerous career opportunities in areas such as government agencies, financial institutions, healthcare organizations, and technology companies. By acquiring the knowledge and skills needed to combat cyber threats, you can position yourself for a rewarding and high-paying career in this field.

Today's man may send and receive any data by email, audio, or video with the press of a button, but has he ever considered how securely his data is being delivered to the other person without any information being leaked? Cybersecurity has the solution. The infrastructure of modern living that is rising the fastest is the internet. Many of the most recent technologies have transformed the face of mankind in today's technological environment. However, because of this new technology, we cannot safeguard our private information, and that's why cybercrime is rising at present.

As more than 60% of total commercial transactions happen online, this field requires a high level of security—the best and most transparent interactions. As a result, cyber-security has recently been a hot topic. The extent of Cyber security is more than just securing the network, and information in the IT business, but also to other industries and various sectors such as cyberspace, etc. Even modern technologies such as cloud computing, mobile computing, E-commerce, and net banking require a high level of security. Because these technologies are important, information about a person's security has become a requirement. Enhancing cyber security and critical information protection infrastructures is critical to the success of any country's security and economic well-being. Even modern technologies such as cloud computing, mobile computing, E-commerce, and net banking require a high level of security. Because these technologies are important, information about a person's security has become a requirement. Enhancing cyber security and critical information protection infrastructures is critical to the success of any country's security and economic well-being.

Given that technical measures alone cannot prevent any crime, law enforcement agencies must be allowed to investigate and prosecute online crimes successfully. Today, many Governments and nations are enforcing strict laws governing cyber security to stop the loss of some significant data. Everyone must also receive training in this cyber and protect themselves from the rise in digital crime.

II. Literature Review

Shi-Jinn Horng et al. used the Support Vector Machine (SVM) technique to develop a new flow for a system that detects intrusions. The proposed system was assessed using the well-known KDD Cup 1999 dataset. When compared to other intrusion detection systems based on the same dataset, this system performed better in the detection of DoS and Probe attacks, as well as overall accuracy.

Mohit Malik et al. In, used a rule-based technique to detect a security attack in a WSN. They identified ten important security attack types and developed a fuzzy rule-based system for calculating the impact of security attacks on the wireless sensor network.

Harmeet Kaurl created a model to reduce network latency and produce end-to-end data promptly. The SPEED protocol was used to simulate a WSN. For analysis, it focused on two different performance parameters: throughput and energy consumption.

Punam Mulak used a hybrid technique that combined the boundary-cutting algorithm and the clustering algorithm. The goal of using this hybrid approach is to improve the accuracy of the intrusion detection system and provide better results than other clustering techniques.

Mohammad Wazid used a hybrid anomaly detection technique combined with k-means clustering. WSNs are simulated using the Optimized Network Engineering Tool (OPNET) simulator, and the resulting dataset consists of traffic data with end-to-end delay data that has been clustered using WEKA 3.6. It was found in this experiment that two types of anomalies, misdirection and black hole attacks, were activated in the network.

Megha Bandgar et al. in, described a novel approach for detecting Internet attacks using Hidden Markov Models (HMM), as well as an intrusion detection system for detecting a signature-based attack. They used a single and multiple HMM model for source separation based on IP and port information from the source and destination.

The authors G. Singh, F. Masseglia, C. Fiot, A. Marascu, and P. Poncelet in [7] addressed the main disadvantage of detecting intrusions through anomaly (outliers) detection. They added a new feature to the unknown behaviors before they are classified as attacks in their work, and they claim that the proposed system guarantees a meager false alarm ratio, making unsupervised clustering for intrusion detection more effective, realistic, and feasible.

Types Of Cyber Attacks

A cyber-attack is the unauthorized use of computer systems and networks. It employs malicious code to modify computer code, logic, or data, resulting in cybercrimes such as information and identity theft.

It is classified mainly into the following categories: -

1. Web-based attack
2. System-based attack

Web-Based Attack: These are the attacks that occur on a website or web application. Some of the important web-based attacks are as follows:

Injection Attack: This is an attack in which some data will be injected into a web application to manipulate the application and fetch the required information. Examples- SQL Injection, Code Injection, log Injection, XML Injection, etc.

I. D.N.S Spoofing

DNS spoofing is a type of cybercrime. When data is introduced into the cache of a DNS resolver, the name server returns an incorrect IP address, diverting traffic to the attacker's computer or any other computer. DNS spoofing attacks can go undetected for long periods and cause serious security problems.

II. Phishing

Phishing is a type of attack that seeks sensitive information such as user login credentials and credit card numbers. It happens when an attacker poses as a reliable entity in electronic communication.

III. URL Interpretation

It is a type of attack in which we can change specific parts of a URL, causing a web server to deliver web pages that he is not authorized to view.

IV. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all the user data.

V. File Inclusion Attacks

It is a type of attack that allows an attacker to gain access to unauthorized or critical files on the web server or to execute malicious files on the web server by utilizing the included functionality

System-Based Attack

These are the attacks that are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows: -

I. Virus: It is a type of malicious software that spreads through computer files without the user's knowledge. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also carry out instructions that are harmful to the system.

II. Worm: It is a type of malware that replicates itself to spread to uninfected computers. It functions similarly to a computer virus. Worms are frequently transmitted via email attachments that appear to be from trusted senders

III. Trojan Horse: It is a malicious program that causes unexpected changes to computer settings and unusual activity, even when the computer should be idle. It deceives the user about its true intent. It appears to be a normal application, but when it is opened/executed, malicious code is executed in the background

IV. Backdoors; It is a method that avoids the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

V. Bots: A bot (short for "robot") is a computer-controlled process that communicates with other network services. Some bot programs run automatically, while others only execute commands when specific input is received. Crawlers, chatroom bots, and malicious bots are common examples of bot programs

Counter-Measures

Boundary firewalls and internet gateways**:** These are devices designed to prevent unauthorized access to or from private networks; however, proper configuration of these devices, whether in hardware or software form, is required for them to be fully effective.

Secure Configuration: Making sure that systems are configured in the most secure manner for the organization's needs.

Access Control: Ensuring only those who should have access to systems, have access and at the appropriate level.

Malware Protection: Ensuring that virus and malware protection is installed, and it is up to date. Downloading software from the internet can expose a device to malware – such as computer viruses, worms, and spyware. Sources of malware include email attachments, downloads, and installation of unauthorized software. Anti-malware scans your files, system, and email, searching for malicious content or behavior. If a system is infected with malware, your organization could experience malfunctioning systems or data loss

Patch Management: Keeping systems up to date is essential, as hackers target older or vulnerable systems. Patch management is the process of managing system and software updates – including how and when they are kept updated, change control, and testing. The WannaCry attack on the NHS in 2017 was due to vulnerabilities in computers that had not applied a recent patch update from Microsoft. Once exploited, software was installed that encrypted all user files and demanded payment for them to be unlocked

Strong passwords: Strong passwords are essential for online account security. Passwords must be at least 12 characters long and contain a combination of upper and lowercase letters, numbers, and symbols

Multi-factor authentication (MFA): MFA adds an extra layer of security to online accounts by requiring users to enter a code from their phone in addition to their password when they log in

Security Software: Antivirus and anti-malware software, for example, can help protect computers from malware and other cyber threats

Security Awareness Training: Individuals can benefit from security awareness training to learn about cyber threats and how to avoid them.

III. Conclusion

Cybersecurity is a critical concern for both individuals and organizations. Cyberattacks can have a significant impact on both personal and professional lives in the increasingly interconnected world of today. This paper tries to explain the various cyberattacks and security methods that can be used to keep our devices from being attacked. It also aids in closing several gaps in their computer operation.

IV. Future Scope

The future of cybersecurity is complex and difficult, but emerging technologies such as AI and machine learning have the potential to significantly improve it. To keep organizations safe, new security standards and frameworks are being developed. Furthermore, there is a growing understanding of the significance of cybersecurity education and training. Individuals and organizations can reduce future risks by remaining vigilant and taking steps to protect themselves from cyberattacks.

References

[1] Shi-Jinn Horng, Ming-Yang Su, Yuan-Hsin Chen, Tzong-Wann Kao, Rong-Jian Chen, Jui-Lin Lai, Citra Dwi Perkasa, “A novel intrusion detection system based on hierarchical clustering and support vector machines”, Elsevier Computer Network, pp.306–313, 2010.

[2] Mohit Malik, Namrata Kapoor, Esh Naryan, Aman Preet Singh, “Rule-Based Technique detecting Security attack for Wireless Sensor Network using fuzzy logic”, International Journal of Advanced Research in Computer Engineering & Technology, Vol. 1, No. 4, ISSN: 2278–1323, June 2012.

[3] Harmeet Kaur, Ravneet Kaur, “Crossbreed Routing Protocol for SPEED Terminology in Wireless Sensor Networks”, International Journal of Advance Research in Computer Science and Management Studies, Vol. 2, No. 7, ISSN: 2321-7782, July 2014.

[4] Punam Mulak, Nitin R. Talhar, “Novel Intrusion Detection System Using Hybrid Approach”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, No. 11, ISSN: 2277 128X, November 2014.

[5] Mohammad Wazid, “Hybrid Anomaly Detection using K-Means Clustering in Wireless Sensor Networks”, Center for Security, Theory and Algorithmic Research, pp. 1-17, 2014.

[6] Megha Bandgar, Komal Dhurve, Sneha Jadhav, Vicky Kayastha, Prof. T.J Parvat, “Intrusion Detection System using Hidden Markov Model (HMM)”, IOSR Journal of Computer Engineering (IOSRJCE) eISSN: 2278-0661, p- ISSN: 2278- 8727Vol. 10, No. 3, pp. 66-70, Mar. - Apr. 2013.

[7] G. Singh, F. Masseglia, C. Fiot, A. Marascu and P. Poncelet, “Data Mining for Intrusion Detection: from Outliers to True Intrusions”, The 13th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD’09), Thailand, 2009.

[8] J. Blackburn and G. Waters, Optimising Australia's Response to the Cyber Challenge, 2011.

[9] L. Bennett, "Cyber security strategy", ITNOW, vol. 54, no. 1, pp. 10-11, 2012.

[10] M. Qiu, L. Zhang, Z. Ming, Z. Chen, X. Qin, and L. Yang, "Security-aware optimization for ubiquitous computing systems with SEAT graph approach", J. of Computer and Syst. Sci., vol. 79, no. 5, pp. 518-529, 2013.

[11] M. Gallaher, A. Link, and B. Rowe, Cyber Security: Economic Strategies and Public Policy Alternatives, Edward Elgar Publishing, 2008.

[12] F. Pasqualetti, F. Dorfler and F. Bullo, "Attack detection and identification in cyber-physical systems", IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715-2729, 2013.

[13] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications", IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 998-1010, 2012.

[14] Tonge, S. Kasture and S. Chaudhari, "Cyber security: challenges for society-literature review", IOSR Journal of Computer Engineering, vol. 2, no. 12, pp. 67-75, 2013. Sharma, Richa and Kumar, Gireesh. "Availability Modelling of Cluster-Based System with Software Aging and Optional Rejuvenation Policy" Cybernetics and Information Technologies, vol.19, no.4, 2019, pp.90-100. https://doi.org/10.2478/cait-2019-0038

[15] G. Kumar and R. Sharma, "Analysis of software reliability growth model under two types of fault and warranty cost," 2017 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, 2017, pp. 465-468, doi: 10.1109/ICSRS.2017.8272866.

[16] Kumar, G., Kaushik, M. and Purohit, R. (2018) "Reliability analysis of software with three types of errors and imperfect debugging using Markov model," International journal of computer applications in technology, 58(3), p. 241. doi: 10.1504/ijcat.2018.095763.

[17] Sharma, R. and Kumar, G. (2017) "Availability improvement for the successive K-out-of-N machining system using standby with multiple working vacations," International journal of reliability and safety, 11(3/4), p. 256. doi: 10.1504/ijrs.2017.089710.