International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 4 ǁ 2022 ǁ PP. 15-17

Literally Survey on Cyber Attack Security and various algorithm

F.Mashiya Afroze, Research Scholar, Dr.Tamilselvi JebaMalar

Abstract

Now a days, usage of Internet has become mandatory for all our day today life. Emerge of technologies has both advantage and disadvantage. All sectors are now online and many vital data are now readily available to hacker online. It has given a path to the hacker to play between User and Service provider. [1]. A proper technique is required to detect and prevent the hacker's attack over online transaction. In this paper a survey about various attack and their causes are discussed.[2]. In the last few years a large number of internet users are increasing additionally different companies, banks and service providers are providing services online. So various sensitive and financial data are becomes online now in these days. This aspect of internet users are an evolution for us but the dark side of this advantage is too hard to accept, because of hackers and intruders are working between end clients and service providers. A secure and efficient technique is required to detect and prevent the attacks over the network transaction.

In this paper a survey about various attacks and their problems is done, which leads to establish a problem statement for finding the optimum solution for the problem arises. In addition of that here we propose a system architecture for future simulation of security in internet based security.

Keyword - *Cyber-attack, Machine Learning Methodology*

Date of Submission: 02-04-2022 Date of acceptance: 16-04-2022

I. Introduction

A cyber attack is a strike against a computer system, network, or internet-enabled application or device. Hackers use a variety of tools to launch attacks, including malware, ransom ware, exploit kits, and other methods. Cyber attacks have been growing at an alarming rate – in volume, sophistication and impact.[3].

II. Areas

1. Credit card theft.

2. Cyberterrorism.
3. Electronic bullying and stalking.
4. Hacking for fun.
5. Identity theft.
6. Network intrusions.
7. Software piracy
8. Hacking.
9. Virus Dissemination
10. Computer vandalism
11. Denial of Service attack.
12. Spam

III. Learning Methodology

There are 3 types of Machine Learning Methods..

1. Supervised Learning - This algorithm consist of a target / outcome variable (or dependent variable) which is to be predicted from a given set of predictors (independent variables). Using these set of variables, we generate a function that map inputs to desired outputs. The training process continues until the model achieves a desired level of accuracy on the training data. Examples of Supervised Learning: Regression, Decision Tree, Random Forest, KNN, Logistic Regression etc.

2. Unsupervised Learning - In this algorithm, we do not have any target or outcome variable to predict / estimate. It is used for clustering population in different groups, which is widely used for segmenting customers in different groups for specific intervention. Examples of Unsupervised Learning: Apriori algorithm, K-means.

3. Reinforcement Learning - Using this algorithm, the machine is trained to make specific decisions. It works this way: the machine is exposed to an environment where it trains itself continually using trial and error. This machine learns from past experience and tries to capture the best possible knowledge to make accurate business decisions. Example of Reinforcement Learning: Markov Decision Process.[4]

IV. Assement

S. No	Type of Cyber Attack	Description	Algorithm / Techniques	Techniques / Reference
1	**Distributed Denial of Service attack (DDoS)**	This happens when a server is overloaded with connections, with a goal of ultimately shutting down the target's website or network system.	New Cracking Algorithm	This algorithm protects legitimate traffic from a huge volume of DDOS traffic when an attack occurs.**[5]**
2	**Bonnets**	Bonnets are the millions of systems infected with malware under hacker control in order to carry out DDoS attacks.	dos	The survey classifies the botnet research into three areas: understanding botnets, detecting and tracking botnets, and defending against botnets.**[6]**
3	**Smurf attack**	This attack involves using IP spoofing and the ICMP to saturate a target network with traffic.	Dos TCP dump from DARPA98 dataset is used	In this paper, principal component analysis method is used for feature selection and dimension reduction.[7]
2	**Phishing attacks**	Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something.	Phishing a new end-host based anti-phishing algorithm, which we call LinkGuard	Implementation of Link Guard in Windows XP. Experiments verified that LinkGuard is effective to detect and prevent both known and unknown phishing attacks with minimal false negatives. [8]
3	**Malware**	Malicious software can be described as unwanted software that is installed in system without your consent. It can attach itself to legitimate code and Propagate	Novel malware methods	analyzation and classification - state-of-the-art malware techniques and their countermeasures.[9]
3a	**Spyware**	Spyware is a type of program that is installed to collect information about users, their computers or their browsing habits	keylogger spyware,	Proposed a framework for detection and prevention of novel keylogger spyware attack. [10]
3b	**Ransom ware**	Malware that prevents or restricts user from accessing their system, unless a ransom is paid.	monitoring - Algorithms	The analysis shows that there has been a significant improvement in encryption techniques used by ransomware. [11]
4	**Eaves dropping attack**	Eavesdropping attacks occur through the interception of network traffic.	amplify-and-forward (AF) protocol decode-and-forward (DF) protocol	In this paper, we investigate security issues in a collaborative wireless network in the presence of eavesdropping attacks, where multiple amplify-and-forward (AF) relays are exploited to secure the message transmission between legitimate users. [12]
5	**SQL injection attack**	A successful SQL injection exploit can read , modify, execute and issue Command to data base	exhibited a novel scheme that automatically transformed web applications	Typical SQL injection attack and prevention technologies are introduced in the paper. The detecting methods not only validate user input, but also use type-safe SQL parameters. SQL injection defense model is established according to the detection processes, which is effective against SQL injection vulnerabilities.[13]
6	**Cross-site scripting (XSS) attack**	XSS attacks use third-party web resources to run scripts in the victim's web browser.	Experiments are conducted on a testbed with the aim to reveal the behavior of the attack.	This paper investigates the XSS attack recognition and detection using regular expression pattern matching and a preprocessing method.[14]
7	**Session hijacking**	The attacking computer substitutes its IP address for the trusted client	Man in middle	This paper categorizes mitigation techniques in terms of strengths

		while the server continues the session, believing it is communicating with the client.	SHA mitigation techniques	and weaknesses, the gaps and areas of improvements. [15]
8	**Spear phishing attacks**	Spear phishing is a very targeted type of phishing activity	Phishing We evaluate and compare the spear phish feature detection attributes with PhishTank, a benchmark dataset.	In this paper, we direct our survey in finding extrinsic porches influential to nasty invasions as attack entry point analysis. [16]
9	**IP Spoofing**	IP spoofing is used by an attacker to convince a system that it is communicating with a known, trusted entity and provide the attacker with access to the system.	Man in middle Hop Count Filtering (HCF) technique	We propose an algorithm, inspired by the Hop Count Filtering (HCF) technique, that changes the learning phase of HCF to include all the possible available Hop Count values.[17]

V. Research Finding

Despite the prevalence of cyber attacks, Check Point data suggests that 99 percent of enterprises are not effectively protected. However, cyber attacks are preventable. The key to cyber defense is an end-to-end cyber security architecture that is multilayered and spans all networks, mobile, and cloud. With the right architecture, you can consolidate management of multiple security layers, control policy through a single pane of glass.

VI. Conclusion

Due to market uncertainties, declining economic growth and significant growth of online e-commerce makes fraud widespread. This paper reviewed types of Cyber attacks and Various machine learning algorithms. This paper also highlighted the description of Cyber attacks and limitations involved with machine learning techniques for secured e- activities. The findings show that algorithms applied in various attacks were found to be effective in terms of authentication. As a future work, the performance of the appropriate machine learning techniques will be implemented in order to avoid the cyber crime in any means.

References

[1]. http://dst.gov.in/basic-research-cyber-security

[2]. A. Ghosh, J. Wanken, and F. Charron. Detecting Anomalous and Unknown Intrusions Against Programs. In Proceedings of the Annual Computer Security Application Conference (ACSAC'98), pages 259-267, Scottsdale, AZ, December 1998.

[3]. Pangalos, G., et al.: The Importance of Corporate Forensic Readiness in the information security framework. In: 2010 Workshops on Enabling Technologies (2010)Google Scholar

[4]. Saeed Abu-Nimeh, Dario Nappa, Xinlei Wang, Suku Nair, “A comparison of machine learning techniques for phishing detection” in Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit

[5]. V.Priyadharshini, Dr.K. Kuppusamy “Prevention of DDOS Attacks using New Cracking Algorithm “, in International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622

[6]. Zhaosheng Zhu, Guohan Lu, Yan Chen, Zhi Judy Fu, Phil Roberts, Keesook Han,” Botnet Research Survey” in 2008 32nd Annual IEEE International Computer Software and Applications Conference

[7]. Gholam Reza Zargar, Peyman Kabiri, “Identification of Effective Network Features to Detect Smurf Attacks” in 2009 IEEE Student Conference on Research and Development (SCOReD)

[8]. Juan Chen ; Chuanxiong Guo, “Online Detection and Prevention of Phishing Attacks”, in International Conference on Communications and Networking in China

[9]. Rahul Raveendranath,Venkiteswaran Rajamani, Anoop Joseph Babu, Soumya Kanti Datta,” Android malware attacks and countermeasures: Current and future directions”, in 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)

[10]. Mohammad Wazid, Avita Katal, R.H. Goudar, D.P. Singh, Asit Tyagi, Robin Sharma, Priyanka Bhakuni,” A framework for detection and prevention of novel keylogger spyware attacks”, in 7th International Conference on Intelligent Systems and Control (ISCO)

[11]. Jinal P Tailor, Ashish D Patel, “A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control”, in International Journal of Scientific Research 4(VIS) · June 2017

[12]. Yulong Zou ; Xianbin Wang ; Weiming Shen,”Eavesdropping attack in collaborative wireless networks: Security protocols and intercept behavior” in Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD)

[13]. Li Qian ; Zhenyuan Zhu ; Jun Hu ; Shuying Liu,”Research of SQL injection attack and prevention technology” inInternational Conference on Estimation, Detection and Information Fusion (ICEDIF) 2015

[14]. M. Ridwan Zalbina ; Tri Wanda Septian ; Deris Stiawan ; Moh. Yazid Idris , Ahmad Heryanto, Inderalaya,” Payload recognition and detection of Cross Site Scripting attack” in International Conference on Anti-Cyber Crimes (ICACC)

[15]. Enos Letsoalo , Sunday Ojo ,” Session hijacking attacks in wireless networks: A review of existing mitigation techniques”, in IST-Africa Week Conference (IST-Africa)

[16]. Deepali N. Pande ; Preeti S. Voditel, “ Spear phishing: Diagnosing attack paradigm” in International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)

[17]. Ayman Mukaddam ; Imad Elhajj ; Ayman Kayssi ; Ali Chehab, “ IP Spoofing Detection Using Modified Hop Count”, in EEE 28th International Conference on Advanced Information Networking and ApplicationsI