TEST Engineering & Management

January-February 2020
ISSN: 0193-4120 Page No. 10488 - 10492

An Automatic Method to Prevent Cybercrime Incidents using Artificial Intelligence Approach

[1]M. Hemanth Reddy, [2]A. Gayathri, [3]N. Deepa

[1]*UG Scholar, Dept. of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India*

[2]*Associate Professor, Dept. of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India*

[3]*Assistant Professor, Dept. of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India*

[1]*gayathribala.sse@saveetha.com*, [2]*hemanth.matli@gmail.com*, [3]*deepa23narayanan@gmail.com*

Article Info
Volume 82
Page Number: 10488 - 10492
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 19 February 2020*

Abstract

As hackers get smarter and more determined, artificial intelligence is going to be an important part of the solution. As corporations struggle to fight off hackers and contain data breaches, some are looking to artificial intelligence for a solution. They're using machine learning to sort through millions of malware files, searching for common characteristics that will help them identify new attacks. They're analyzing people's voices, fingerprints and typing styles to make sure that only authorized users get into their systems. And they're hunting for clues to figure out who launched cyber-attacks and make sure they can't do it again. Presenting successful and profoundly progressed digital guard frameworks has gotten basic. Starting today, with the innovation, the globe is moving towards the man-made brainpower (AI). Computer based intelligence assumes a significant job in innovation and has been engaged with numerous mechanical angles also. Making digital safeguard frameworks, utilizing astute operators has become a pattern by today. Fundamentally, a canny operator is a product segment which can be developed in a situation, take choices, and has the capacity of seeing and speaking to. The reason for this investigation is to present a modern digital wrongdoing resistance framework which includes wise specialists that depend on man-made reasoning.

Key Words: *Disseminated assault recognition, appropriated secure estimation, sticking assault, bogus information infusion assault, and remote sensor arranges.*

1. Introduction

This exploration paper for the most part centers around how to battle cybercrimes, and furthermore it shows how insightful and powerful the apparatus "operator" that can be utilized in recognition and anticipation of digital assaults. Digital assaults will in general hugy affect the IT business with regards to information burglary, numerous social orders over the world have parts or frameworks which rely upon web applications. As web applications are utilized progressively on essential and basic exercises they have become a truly powerless and a prominent Objective for

January-February 2020
ISSN: 0193-4120 Page No. 10488 - 10492

security assaults. It tends to be seen that the expansion of digital assaults are extremely high in the present the internet. Any activity that sidesteps the security components of the focused on framework utilizing a PC and a system can be characterized as a cybercrime. In a cybercrime the PC may be utilized as a gatecrasher or it tends to be the objective. In the internet looking after classification, respectability and accessibility are fundamental. Most system driven digital assaults are completed by shrewd operators, for example, PC worms and infections; consequently, battling them with canny semi-independent specialists that can distinguish, assess, and react to digital assaults has become a prerequisite.

Physical gadgets and human intercession are not adequate for observing and assurance of these frameworks from assaults. Accordingly, the investigation of digital assault location techniques and frameworks are turning into a famous and fascinating subject among the authorities with regards to the system security field. Extensions of the interruption frameworks are quick in present day innovative condition. Interruption discovery frameworks (IDS) are one of the extremely well known frameworks which are sent to recognize digital assaults. It very well may be named have based frameworks or system based frameworks. Host-put together frameworks are based with respect to data's of a solitary host while organize put together frameworks are based with respect to checking traffic of the data. It is important that these digital resistance frameworks being adaptable, versatile and incredible, and having the option to identify a wide assortment of dangers and settling on clever continuous choices. Aside from IDS's, Intrusion Prevention Systems (IPS) is likewise being utilized in this innovation. These won't just recognize and caution about digital assaults yet will keep them from going into the framework. IPS's are set in-line and can effectively forestall/square interruptions that are recognized, all the more explicitly IPS can accept such activities as sending an alert, dropping the vindictive bundles, resetting the association as well as hindering the traffic from the culpable IP address which could be extremely irksome for the digital assailants and enthusiastic for the clients. An Agent is a little program module that capacities persistently and independently. Attributes of an operator framework ought to be reactivity, proactive in real life and little in size. There are numerous points of interest of building cybercrime discovery frameworks utilizing the specialist innovation.

2. Literature Review

Contrasted with the past, improvements in PC and correspondence innovations have given broad and propelled changes. The use of new advancements give incredible advantages to people, organizations, and governments, be that as it may, it messes some up against them. For instance, the protection of significant data, security of put away information stages, accessibility of information and so on. Contingent upon these issues, digital fear based oppression is one of the most significant issues in todays world. Digital dread, which made a great deal of issues people and foundations, has arrived at a level that could undermine open and nation security by different gatherings, for example, criminal associations, proficient people and digital activists. In this way, Intrusion Detection Systems (IDS) have been created to maintain a strategic distance from digital assaults. In this examination, profound learning and bolster vector machine (SVM) calculations were utilized to recognize port sweep endeavors dependent on the new CICIDS2017 dataset and 97.80%, 69.79% exactness rates were accomplished individually.

January-February 2020
ISSN: 0193-4120 Page No. 10488 - 10492

Digital assaults can truly influence the security of PCs and system frameworks. In this way, building up a productive abnormality discovery system is essential for data assurance and digital security. To precisely identify TCP SYN flood assaults, two factual plans dependent on the constant positioned likelihood score (CRPS) metric have been planned in this paper. In particular, by incorporating the CRPS measure with two traditional outlines, Shewhart and the exponentially weighted moving normal (EWMA) diagrams, novel abnormality recognition methodologies were created: CRPS-Shewhart and CRPS-EWMA. The proficiency of the proposed techniques has been confirmed utilizing the 1999 DARPA interruption identification assessment datasets.

3. Proposed System Design

Social building is a very regular strategy for misleading individuals in the Cyberspace. Phishing is one of the most widely recognized assaults that the social specialists use to deceive the clients to uncover their classified data. While different kinds of security plans and Intrusion Detection Systems (IDSs) might be utilized to relieve different sorts of digital assaults, phishing can't be impeded uniquely by utilizing those, regardless of whether the procedures are complex. This is on the grounds that, frequently the human slip-ups are associated with the procedure of spillage of secret information and data.

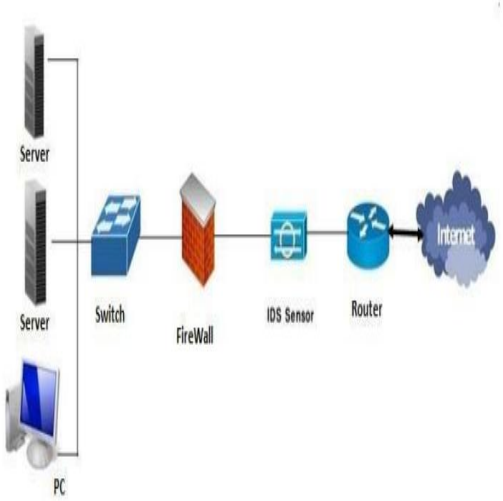

Figure 1.1: Process of Internet and server communication

Henceforth, familiarity with the issue and controlled digital conduct would be vital to shielding against phishing type assault. Another digital assault, Cross-Site Scripting (XSS) could likewise be handled proficiently by utilizing some Content Security Policy (CSP) which would work nearby the generally utilized security and barrier systems. The motivation behind this discussion is to share some examination discoveries in these and significant zones. Additionally, some data would be shared for the general perusers of the subject. We might want to investigate how the significant part of these kinds of assaults could be upset or alleviated just by watching a few safety measures while communicating in the Cyberspace.

4. Result and Discussion

As of late the web is being begun to be presented in each part of our lives during the time spent digitalization. With this improvement works, the web is ending up being one of the center essentials of regular day to day existence. Other than the benefits, it is showing a few bad marks simultaneously. In spite of the fact that the advancements are being produced

January-February 2020
ISSN: 0193-4120 Page No. 10488 - 10492

for genuine purposes, the use of them for unsafe reasons for existing is expanding essentially.

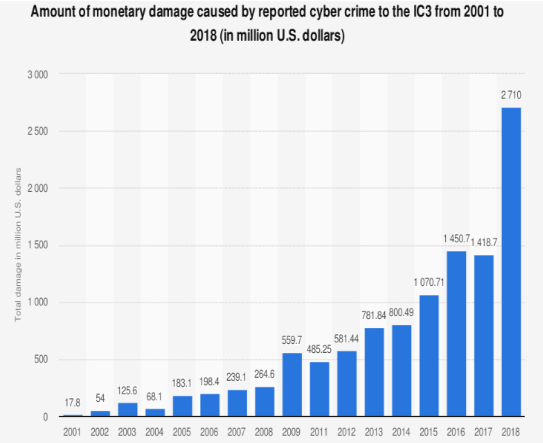

Figure 1.2: Damage caused by reported cybercrime accuracy level

These wrongdoings can make significant effects on our general public dependent on the degree of seriousness. Since cybercrime happens through the cutting edge specialized gadgets utilizing web associations, it is naturally an extremely convoluted assignment to recognize the wrongdoing and distinguish the guilty party. In this paper, a system for both programmed and manual strategies have been proposed to identify cybercrime and accuse the guilty party of evidence.

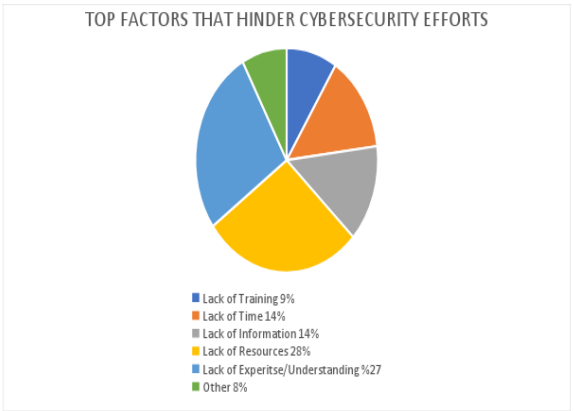

Figure 1.3: Analysis if Cyber Security efforts

5. Conclusion

As we live in a modernized world, the greater part of our regular interchanges and business exercises occur by means of the Internet. Nonetheless, it additionally causes issues which are difficult to deal with, for example, the development of digital assaults on PC systems. Within reach scholarly assets show that AI techniques as of now have different execution to handle cybercrimes. This paper compactly presented conceivable outcomes of AI methods so far in digital field for battling digital wrongdoings and their present restrictions. With the improvement of innovation step by step programmers are additionally developing savvy. May be in future programmers additionally attempts to utilize the different methods for man-made reasoning to break into system or framework.

Reference

[1] Cheshta Rani, Shivani Goel. An Expert System for Cyber Security Attack Awareness, International Conference on Computing, Communication and Automation (ICCCA2015) ISBN:978-1-4799-8890-7/15/$31.00 ©2015 IEEE 242 CSAAES.

[2] A. S. Poonia, A. Bhardwaj, G. S. Dangayach, (2011) "Digital Crime: Practices and Policies for Its Prevention", The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management, Vol. 19, No. SP1.

[3] Dr. Sunil Bhutada, Preeti Bhutada. Applications of Artificial Intelligence in Cyber security International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, April 2018 All Rights Reserved © 2018 IJERCSE 214 .

[4] Nikita Rana, Shivani Dhar,Priyanka Jagdale, Nikhil Javalkar. Execution of An Expert System for the Enhancement of E-Commerce Security International Journal of Advances in Science Engineering and

January-February 2020
ISSN: 0193-4120 Page No. 10488 - 10492

Technology, ISSN: 2321-9009 Volume-2, Issue-3, July-2014

[5] M.M. Gamal, B. Hasan, and A.F. Hegazy, "A Security Analysis Framework Powered by an Expert System," International Journal of Computer Science and Security (IJCSS), Vol. 4, no. 6, pp. 505-527, Feb. 2011.

[6] K. Goztepe, "Planning a Fuzzy Rule Based Expert System for Cyber Security," International Journal Of Information Security Science, vol.1, no.1, 2012.

[7] D. Welch, "Remote Security Threat Taxonomy," Information Assurance Workshop. IEEE Systems, Man and Cybernetics Society, pp 76-83, June 2003.

[8] Vidushi Sharma, Sachin Rai, Anurag Dev" A Comprehensive Study of Artificial Neural Networks" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 10, October 2012.