www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 1 Jan. 2017, Page No. 20011-20016
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i1.31

Usage of Data Mining Techniques for combating cyber security

Farhad Alam[1], Sanjay Pachauri[2]
[1]Research Scholar, Himalayan University, Arunachal Pradesh, India Farhad.alam@email.com
[2]Assistant Professor IMS Unison University, Dehradun(U.K.),
India-248009.

Abstract

Cybersecurity is concerned with protecting computer and network system from corruption due to malicious software including Trojan horses and virus. Security of our network system is becoming imperative as massive sensitive information is transmitted across the network. In this research paper, data mining application for cybersecurity is highly explored. We discussed various cyber-terrorism or attack committed across the network such as malicious intrusion, credit card fraud, identity thefts, and infrastructure attack. Data mining techniques such as classification, anomaly, link analysis and soon are being applied to detect or prevent the aforementioned cyber-terrorism or attack. Recommendations were made and suggestions for further study was indicated are amazingly valuable in finding security breaks.

1. INTRODUCTION

Cyber security consists of security mechanism that attempt to provide solutions to cyberattacks or cyber-terrorism. Security of network systems is becoming increasing important as more and more sensitive information is being manipulated and stored online. as a consequence, the integrity of computer networks, bothering relation to security and regarding to the nation of institutional life in general is a growing concern. According to Security intelligence reports that cybercrime wave around the world is worrisome. According teethe U.S FederaleTrade commissions (FTC) credit card fraud cost card issuers and holders hundreds of millions of dollars every year which create a huge damage to the economy. Loathe biennial department of trade and industry (DTI) security breaches survey reports stipulated that around 70% of UK business had a computer security crime incident in 2016. additionally, security and defense networks, intellectual property, proprietary research, and data based market mechanisms that depend on hindered and undistorted access, can all be personally additionally, security and defense networks, intellectual property, proprietary research, and data based market mechanisms that depend on hindered and undistorted access, can all be personally

Compromised by malicious intrusions. There is a need to use the best way to protect these systems. That is an effective way is needed to find the security breaches. Data mining has many applications in security includes in national security (e.g. Surveillance) botnet detection, as well as in cyber security (like virus detecting). Data mining or knowledge discovery (KDD) is a method which uses to analyze data from a target to source (like in data warehouse) and compose that feedback into useful information. Data mining techniques are used to find the patterns of suspicious individuals and groups, and to search which individuals and groups area able to achieve terrorist activities. Data mining can also help healthcare insurers to detect fraud and abuse.

In this study, we will mainly focus on Data mining application to protect cyber security. To get the mechanism to be adopted in order to protection the nation's computers and network, it is important to understand the types of threats that put at risk the cyber network. Against this backdrop, this paper discusses about cyber terrorism, malicious intrusions threats and external attacks, as well as fraud credit card identification. We were also discussed attacks on a critical infrastructure. Finally, we discussed about data mining application for cyber security and suggestions for further study was made

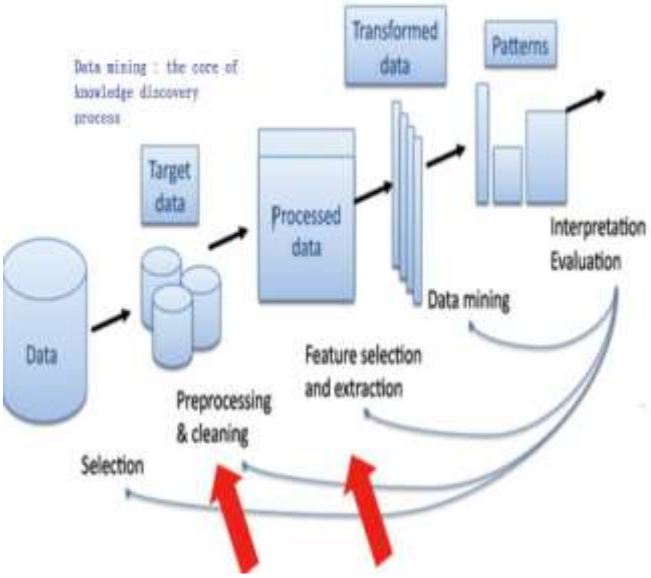
Data mining : the core of knowledge discovery process
Transformed data
Patterns
Target data
Processed data
Interpretation Evaluation
Data mining
Data
Feature selection and extraction
Preprocessing & cleaning
Selection

Figure of KDD Process.

2. Cyber-Terrorism, Threats and External Attacks

2.1. Overview

Cyber-terrorism, according to the O' Leary (2010) is committed through the use of cyberspace or computer resources. Cyber-terrorism is one of the major terrorist threats posed to our nation today. This threat escalated as a result of vast information transmitted electronically across the web. Attacks on our computers, networks, internet intra-structure and databases could be devastating to the business. It is estimated that cyber – terrorism could cause billions of dollars loss to businesses. A classic example is that of a banking information system. According Reserve Bank of India (RBI), for all internets related complaints received 20% of cases involved a bank account debit and misuse of account numbers.

If terrorist attack such a system and deplete accounts of funds, then the bank could lose millions or billions of moneys. Crippling the computer system millions of -hours of productivity could be a lost, which is Ultimately equivalent to moneyless. Even a simple power failure at work through some accident could cause several hours of productivity loss which leads to financial loss. Therefore, it is imperative that our information system could be secured.

Threats can happen from inside or outside the association. Outside assaults are assaults on PC system from somebody outside the association. Saltines can break into the PC system and cause a ton if destruction inside the association. A few saltines spread infection that harm records in different PC systems. In any case, the all the more destroying one is that of within risk. These individuals are frequently under bolted, yet they are the general population who comprehended the essential information in the association. Individuals inside an association who have concentrated on the business practices and strategies have a huge point of interest when creating plan to handicap the association's information resources. These individuals might be consistent representatives or even those working at the PC focuses. The issue is exceptionally crushing as somebody masquerades as another person, and causes a wide range of harm, for example, taking vital specialized information or presenting what is known as a "bomb" that is a ruinous PC program into the system. Whatever is left of the paper will inspect how information mining could be utilized to counteract such assaults.

2.2. Malicious Software and Malicious Intrusion

Malicious software is programs particularly intended to harm or upset a PC system (O' Leary 2010). The most well-known sorts of these projects are infections, worms and Trojan steeds and are ordinarily engendered to the PC system through Hackers and saltines. The objective of noxious interruptions incorporates systems, web customers and servers, working system and database. Numerous digital terrorism is because of pernicious interruptions. We hear much about of system interruptions. What happens here is that the interlopers attempt to take advantage of the systems and get indispensable information that is being transmitted. These interlopers might be human gatecrashers or computerized noxious programming set by people. Interruption can likewise target records within system correspondences. Case in point, an aggressor can take on the appearance of a true blue client and utilize their qualifications to sign in and access confined documents. Malignant interruption can likewise happen on databases, at times, stolen certifications empower the aggressor to posture inquiries, for example, SQL questions and get to confined information.

In discussing malicious intrusion or cyber-attacks it is often helpful to draw analogies from the noncyber world (that is non-information related terrorism) and then translate those attacks to attacks on networks and computers. For instance, a thief could enter in a building through a door. In the same way, a computer intruder could enter the computer or network through some sort of a trap door that has intentionally build by a malicious insider and left unattended perhaps through careless design.

In the case of credit card fraud, which is a our serious problem too, here an attacker obtains a person’s credits card information and uses it to make unauthorized purchases. By the time the owner of the card becomes aware of the fraud; it may be too late to reverse the damage or apprehend the culprit. A similar problem occurs when using ATM card on Automated Teller Machine (ATM) in withdrawing money from the bank. Thus, there is a need to explore the use of data ining for both credit card and detection and as well es identity theft.

2.3. Critical Infrastructures Attack

Attack on critical infrastructure is extremely hazardous in light of the fact that this could handicap a country and its economy. Infrastructure assaults comprise of assaulting telecom lines, power, power, gas, repositories and water supplies,

DOI: 10.18535/ijecs/v6i1.31

nourishment supplies and other fundamental civilities that are foremost for the operation of the country.

Critical infrastructure assaults could happen amid an assault whether they are information related, noninformation related or bio terrorism assault. For example, one could assault the product that runs the information transfers industry and close down all the telecom lines. Telecom lines could likewise assault physically through bombs and dangerous chemicals. So also, programming that runs the force and gas supplies could be assaulted. Assault on infrastructure could likewise happen in transportation line, for example, assaulting railroads and high ways.

All these could bring about a considerable measure of harms in the event that it is not ensured.

Besides, infrastructures could likewise be assaulted by normal fiasco, for example, tropical storms and quakes. Be that as it may, our primary enthusiasm here is the assaults on infrastructures through vindictive assaults, both information and noninformation related. The principle objective of the scientists is to apply information mining to counteract or identify such infrastructure assaults

2.4. Data Mining Application for Cyber Security

Data mining According to Sill tow (2012) automates the location of significant examples in a database, utilizing characterized methodologies and calculations to investigate present and verifiable information that can then be broke down to anticipate future patterns. Since information mining devices foresee future patterns and practices by perusing through database for shrouded designs, they permit associations to make proactive, learning driven naughty and answer addresses that were already too tedious to determine.

Data Mining application for digital security is the utilization of information mining strategies to identify digital security. Information mining is being connected to issues territories, for example, interruption discovery and inspecting. For example, in abnormality recognition procedures, it could be utilized to recognize common examples and practices. As indicated by Thuraisingham, Khan and masud (2013) information mining arrangement method might be utilized to bunch different digital assaults when it happens.

Join examination might be utilized to follow self-spreading noxious code to its writers. Expectation information mining strategy might be use to decide potential future assaults depending in a path on information learnt about terrorists through our e telephone discussions and email. In addition, in the utilization of information digging for digital security, non-genuine information mining might be evoking or apply to a few dangers while for certain other risk constant information mining might be utilized, for example, as a part of Network interruption where ongoing information mining might be connected to recognize misrepresentation. As indicated by Thuraisingham, and etal (2013) they stipulated again that continuous information digging might be utilized for Master Card misrepresentation location as it is advising of ongoing preparing, that it is basic that the outcome and the models fabricate ought to be created progressively. Be that as it may, the models are normally worked early. Despite the fact that building model progressively might challenge. Information mining can likewise be utilized for investigating web logs, here base on the consequences of information mining apparatus one can figure out if any unapproved interruptions have happened.

Data Mining application for digital security different regions incorporate into the examination of review information. Here one could construct a distribution center or store containing the review information and after that direct an investigation utilizing different information mining instruments to see whether there is a potential oddity.

For instance, there could be a circumstance when a man has been getting to the information base between the hours of 3-4am yet throughout the previous 2 days he has gotten to database between the hours of 3-4pm. This could then be labeled as an uncommon example that could be need legitimate examination to know whether if an unapproved question has been postured on the database. Moreover, insider danger examination is likewise an issue from a digital security. Insider risk are those worker working in a company who are thought to be trusted could submit surveillance. Additionally, the individuals who have legitimate access to the PC system could plant infection and Trojan stallions and to gets such terrorist will be exceptionally troublesome than getting terrorists outside the association. As a consequence of this it is basic that one ought to screen the entrance examples of the considerable number of people of a company regardless of the possibility that they are system chairmen to see whether they are completing digital terrorism exercises. Information mining method could be utilized to present delicate relationship from the true blue reactions.

3. Conclusion

In this paper, we had explored different kind of cyberterrorism or attacks such as credit card fraud, identity theft, malicious intrusion, and attack on criticalainfrastructureacommitted on the network that has deterred the integrityaand effectiveness ofacomputer network. These cyber-crimesashould be prevented or detected using datamining technique

4. RECOMMENDATIONSAAND SUGGESTIONS FORAFURTHER STUDY

For all intents and purposes each segment is being digitalized on everyday schedule. There is a propensity for acceleration of delicate, information, transmitted over the system. Accordingly, the security of our system and PC systems must be guaranteed. Information mining strategies ought to be investigated as the hate component to battle digital terrorism or assault. Subsequently, PC or information innovation proficient and non-expert ought to be viably prepared on the utilization of information mining strategies base model as choice system to effectively guarantee the security of our system which would upgrade the benefit possibilities of the whole world economy. The specialist recommends further research on the use of information digging systems for botnet recognition for an intrigued researcher who ran over this work.

DOI: 10.18535/ijecs/v6i1.31

The expression "bot" originates from a word robot. A bot is ordinarily self-governing programming fit for performing certain capacities. A botnet is a system of bots that are utilized by a human administrator or bot expert to carryout malignant activities. Botnets are a standout amongst the most effective devices utilized as a part of digital wrong doing today the most effective devices utilized as a part of digital wrongdoing today as it is equipped for influencing Dos (Denial – of – administration assault), spamming, phishing and listening in on remote PCs. Be that as it may, with the assistance of bonnet, people, business and Government are confronting a great deal of a great many dollars harms. It is central that the digital security group or any intrigued research researcher

ought to proffer an information mining system to battle this test danger.

References

[1].http://www.aaai.org/ojs/index.php/aimagazine/article/viewFile/1230/1131

[2]. Chan, P, et al, “Distributed Data Mining in Credit Card Fraud Detection”, *IEEE Intelligent Systems*, 14 (6), 1999.

[3]. Contel, Bradford (2012). Different types of data mining technique. Follow e wise.com. Retrieved 11th Sept, 2012.

[3]. Silltow, J. (2012). Pattern recognition in data ining. Maryland, U.S.A: University of Maryland College Park.

[4]. Thuraisingham, B., Khan, L., & Masud, M. (2013). Data ining for security Applications. Retrieved 27th January, 2014.

[5]. U.S. Federal Trade Commission (F.T.C) (2012). Survey released. Retrieved March 13, 2012.

[7]. Masud, M. M., Khan, L. and Thuraisingham, B. “Feature based Techniques for Auto-detection of Novel Email Worms”, In *Proc. 11th PacificAsia Conference on Knowledge Discovery and Data Mining (PAKDD 2007)*, Nanjing, China, May 2007, page 205-216.