International Journal of Grid and Distributed Computing
Vol. 13, No. 2, (2020), pp. 261 – 269

Designing of Advance Cyber Security Solution using AI Techniques: WEBSTUXCRY

Namita Parati ,

Research Scholar, Department of CSE, Babasaheb Naik College of Engineering, Pusad, Maharashtra, India.

Dr Salim Y Amdani ,

Department of CSE, Babasaheb Naik College of Engineering, Pusad, Maharashtra, India.

Abstract:

Now a day's cybercrime is an most popular illegal activity executed by an malicious intentioned people or by an group of computer expert peoples with the help of internet as the use of internet is tremendously exploded. The use of worldwide web and frequent use of compute and mobile for the easiness of life leads to magnificent exposure of various cyber attacks (cyber security intrusion) that results a disastrous and grievous situation. This situation becomes a global concern to all over the world as internet is used in every field of work for eg. Medical, security offices, banks educational institution etc. Cyberspace and its related structure and components are more vicious to various security threats of both types physical and cyber threats. In our research we had find various cyber-security domain to find solutions in global standard. So it is necessary to know how to perform various transactions on the internet safely. Everyone is prone to the attack from the cyber criminals. One must be aware and should have knowledge of cybercrime. Everyday an advance technique is evolving in each domain. Our research wok is describes a brief idea the recent emerging advancement in the cyber-security domain which also covered the latest attacks that can be used by the hackers to the individual users those are using internet most regularly for every use. Rest of the paper is structured as follows: Section 1 gives a brief idea of internet infrastructure and threats, followed by literature review section that contains various types of existing threats, then a next section was our proposed approach section followed by an conclusion and future scope section.

Keywords: *Cyber-security, malware, cyber-attack, internet.*

1. INTRODUCTION

Nowadays worldwide web has become the most frequently grown technology in the field of technical infrastructure development and digital communications is a ubiquitous and fastest trend towards the digital world. The prior need of a World Wide Web and connectivity between the devices gives a way of new research where the daily usage products like a vehicle, electronics appliances, mobile phones, etc are integrated with an internet connection so that daily lives become easier. Basically everything like vehicle, electricity electronics appliances military services all depends on internet functionality only. Possibility of use of internet infrastructure is a basic need for creating any network –based services like e-mails, payment of electricity bill, mobile recharges, automatic driven vehicles, any type of online data transfer, online reading, learning ,teaching etc. This network based services proven a very much advantageous to society for becoming a developing society and country.

ISSN: 2005-4262 IJGDC

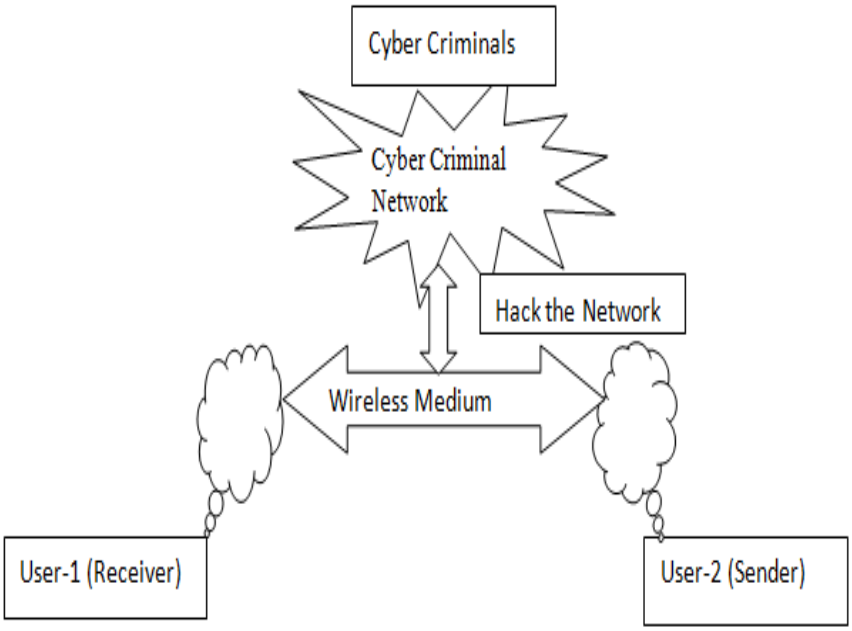

Figure 1. How Cyber Criminal Hack Data

The range of web applications starts from online business, e-govt, education, medical, environmental, to online space mission application etc as they provide sufficient and efficient transmission medium to data transfer for remote to rural areas and very wide coverage range. This services reduces the maximum cost ,time for data transfer that is done by in physical way .For example in earlier days postman was having a responsibility of handling data written in simple page from sender to receiver which was taking a lots of days to be transmitted which is now can bee done with in a second using email services. Also this email services is free of cost with a second of time required to transfer data from any country with in the world even from earth we can transmit data to other planet too which is not possible by using any physical means of data transfer. Given the limited financial resources of many people in developing countries, the Internet enables them to use services they may not otherwise have access to outside the network.. In 2003 alone, malicious software caused damages of up to USD 17 billion.28 By some estimates, revenues from cybercrime exceeded USD 100 billion in 2007, outstripping the illegal trade in drugs for the first time. Nearly 60 per cent of businesses in the United States believe that cybercrime is more costly to them than physical crime. These estimates clearly demonstrate the importance of protecting information infrastructures. Most of the above-mentioned attacks against computer infrastructure are not necessarily targeting critical infrastructure. However, the malicious software “Stuxcry” that was discovered in 2019 underlines the threat of attacks focusing on critical infrastructure. The software, with more than 4000 functions focused on computer systems running software that is typically used to control critical infrastructure.

1.2 CYBER SECURITY AND CYBERCRIME

Cybercrime and cyber security are the most challenging notes which can be avoided when we are talking about an world wide web data services. Securing the internet connection is a major issue in recent development of information technology as well as in internet services. Improving the security of internet connection and important data which is to be shared are the most important research area for every researcher. This securing the web world connection bas becomes most happening topic. Cybercrime has a become a deterring issue in national cyber security cell and internet information protection law. For this an security official can make use some legislation law enforcement for against in any cyber criminal for the misuse of any internet services or accomplishing any illegal activities using internet communication services or using its infrastructure. At the national level, this is a mutual

ISSN: 2005-4262 IJGDC

duty requiring composed activity identified with avoidance, readiness, reaction and recuperation from occurrences with respect to government specialists, the private segment and residents. The plan and execution of a national system and technique for digital security hence requires an extensive methodology. Digital security techniques – for instance, the advancement of specialized assurance frameworks or the training of clients to keep them from turning out to be casualties of cybercrime – can assist with decreasing the danger of cybercrime. The turn of events and backing of digital security procedures are an essential component in the battle against cybercrime. The battle against cybercrime needs a far reaching approach. Given that specialized estimates alone can't forestall any wrongdoing. "Specialized and procedural measures" centers around key measures to advance selection of upgraded ways to deal with improve security and hazard the board in the internet, including accreditation plans, conventions and guidelines. "Authoritative structures" centers around the counteraction, location, reaction to and emergency the executives of digital assaults, including the assurance of basic data foundation frameworks. Cybercrime regularly has a global measurement.

1.3. PHENOMENA OF CYBER CRIME

Cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity.88 There are several difficulties with this broad definition. It would, for example, cover traditional crimes such as murder, if perchance the offender used a keyboard to hit and kill the victim or “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks”. These more refined descriptions exclude cases where physical hardware is used to commit regular crimes, but they risk excluding crimes that are considered as cybercrime.

1.4. TYPOLOGY OF CYBERCRIME

The term “cybercrime” is used to cover a wide variety of criminal conduct.98 As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime.99 One approach can be found in the Convention on Cybercrime which distinguishes between four different types of offences

a. Physical Computer System oriented crimes
b. Information oriented crimes
c. Data-Copyright related crimes
d. Confidential and integrated data related crime.

2. LITERATURE REVIEW

The criminal abuse of information technology and the necessary legal response are issues that have been discussed ever since the technology was introduced. Over the last 50 years, various solutions have been implemented at the national and regional levels. One of the reasons why the topic remains challenging is the constant technical development, as well as the changing methods and ways in which the offences are committed.

2.1. CRIME STATISTICS

The accompanying numbers have been extricated from national wrongdoing measurements. As further talked about underneath, they are not planned to be illustrative of either the worldwide advancement of cybercrime or of the genuine degree of cybercrime at the national level, and are in this way introduced uniquely to give an understanding into nation data.

ISSN: 2005-4262 IJGDC

Sr. No.	Types of Crime	Description
1.	Illegal Access of Data User(Cracking the security and hacking the system) access (hacking, cracking)	1. In this type of crime a non-technical person will hack the user computer system illegally. 2. Its an oldest type of crime
2.	Hacking Data Illegally	1. Sensitive information is often stored in computer systems 2. Attacker tries to acquire access of user 's data through any internet source.
3.	Illegal Interception	1. Attackers may tries to intercept victims personal information or any other important data while data is being transferred between the channel. This type of attack is also known as Information Espionage. 2. Attacker may use different methods to get access of victim's system ,or software to scan victim's data or his various activities.
4.	Information Interference	1. Attack may violate the information integrity and do interference in their activities by erasing, suppressing or modifying some important data.
5.	Computer System Interference	1. Attacker can send some type of worms or malware programs which will effect the working or performance of the victim's system 2. Basically these are the auto-executable porgrams which will Lower down the performance of computer network by creating un-necessary data- transmission.
6.	Spam Threats	1. This word name "SPAM" describes the transmission of unwanted bulk data packets. 2. Most basic example of this type of threat is bulk emails, automatic call through various numbers.
7.	Online Auction Fraud	1. Attackers will accomplishing by using any online auction software so that he can't be distinguished by investigation officer if the victim reports a crime against attacker.
8.	Advance Payment of Fee Fraud	1. This is most basic of crime reporting recently in various cities. Here attacker will ask the victim to enter his bank details to complete the basic registration process by just paying one rupees and then he will use victim's bank details for illegal use .
9.	Computer-Related Forgery	1. Here attacker will manipulate digital documents by hacking the victim's personal data and modifying the information of the documents or making illegal use of victim's data.

ISSN: 2005-4262 IJGDC

10.	Identity Theft	1 Attacker will hack victim's identity without using any technical specification. Here attacker can be in a form of victim's friend or neighbor.
11.	Date of birth, address and phone numbers	1. Such data can in general only be used to commit identity theft if they are combined with other pieces of information

• In India cyber crime cell complaint 25.9% increase in complaints submitted in this year than a last year 2019.

• In Germany crime statistics reports the overall internet related crime has been increased in 2020 by 24.9% than in the year 2019.

Also it is not clear that the represented statistics is 100% correct or not and the data represent reliable information about the crime or not. There are a few challenges related with deciding the worldwide danger of cybercrime based on wrongdoing insights. Above all else, wrongdoing insights are for the most part made at the national level and don't mirror the global extent of the issue. Despite the fact that it would hypothetically be conceivable to join the accessible information, such a methodology would not yield solid data on account of varieties in enactment and recording rehearses. Joining and contrasting national wrongdoing insights requires a specific level of similarity that is missing with regards to cybercrime. Regardless of whether cybercrime information are recorded, they are not really recorded as a different figure. Besides, measurements just rundown wrongdoings that are recognized and reported.161 Especially with respect to cybercrime, there are worries that the quantity of unreported cases is noteworthy.

2.2. SURVEYS

The following numbers have been extracted from different surveys. As further discussed below, they are not necessarily representative, and are thus presented only to give an insight into the results of such surveys.

Credit card and bank account information are among the most popular information advertised on underground economy services. The prices range between USD 0.85-USD 30 (single credit card information) and USD 15-USD 850 (single bank account information).

a. In 2007, auction fraud was among the top Internet scams in the US, with an average loss of more than USD 1 000 per case.

b. In 2005, losses as a result of identity-related offences in the US totalled USD 56.6 billion

c. The financial and personal cost of cybercrime varies significantly among single incidents in Ireland, generating aggregate costs of over EUR 250 000.

d. A single computer security company created more than 450 000 new malicious code signatures in a single quarter.

e. A quarter of all companies responding to a questionnaire in 2010 reported operational losses as a result of cybercrime.

f. Decreasing number of denial-of-service and computer-virus attacks reported by security professionals between 2004 and 2008.

g. In 2009, the United States, China, Brazil, Germany and India were among the countries reporting most malicious activities.

ISSN: 2005-4262 IJGDC

2.3. Types of Cyber-Crime:

Table 1. Types of Cyber Crime Attacks

.

2.4. THE CHALLENGES OF FIGHTING CYBERCRIME

2.4.1. INFRASTRUCTURE

Many everyday communications depend on ICTs and Internet-based services, including VoIP calls or email Communications. Existing technical infrastructure has a number of weaknesses, such as the monoculture or homogeneity of operating systems.

2.4.2. NUMBER OF USERS

The popularity of the Internet and its services is growing fast, with over 2 billion Internet users worldwide by 2020. With the growing number of people connected to the Internet, the number of targets and offenders increases. It is difficult to estimate how many people use the Internet for illegal activities. Even if only 0.1 per cent of users committed crimes, the total number of offenders would be more than one million. Although Internet usage rates are lower in developing countries, promoting cyber security is not easier, as offenders can commit offences from around the world.

2.4.3. AVAILABILITY OF DEVICES AND ACCESS

Only basic equipment is needed to commit computer crimes. Committing an offence requires hardware, software and Internet access. With regard to hardware, the power of computers is growing continuously. There are a number of initiatives to enable people in developing countries to use ICTs more widely. Criminals can commit serious computer crimes with only cheap or second-hand computer technology – knowledge counts for far more than equipment. The date of the computer technology available has little influence on the use of that equipment to commit cybercrimes. Committing cybercrime can be made easier through specialist software tools. Offenders can download software tools designed to locate open ports or break password protection. Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices. The last vital element is Internet access. Although the cost of Internet access is higher in most developing countries than in industrialized countries, the number of Internet users in developing countries is growing rapidly. Offenders will generally not subscribe to an Internet service to limit their chances of being identified, but prefer services they can use without (verified) registration. A typical way of getting access to networks is the so-called “wardriving”. The term describes the act of driving around searching for accessible wireless networks. The most common methods criminals can use to access the network fairly anonymously are public Internet terminals, open (wireless) networks hacked networks and prepaid services without registration requirements.

3. PROPOSED TECHNIQUE FOR PREVENTING EXTERNAL THREAT TO THE INFRASTRUCTURE

“Stux” is a type of malware i.e. an intended software which encrypts all the data and information on a computing device thus leading the stored data and information inaccessible to the system for the user using that system hence the system will become useless for the current user. And then the attacker will then use good identity and will ask the victims for helping them in decrypting the message by providing them a decryption key with some ransom amount to be payed for that decryption key. As the attacker is using fake id for the decryption process it is not guaranteed that after paying the decryption of data

ISSN: 2005-4262 IJGDC

processing fee attacker will decrypt or will not decrypt the victim's data. Fig (3.1) shows the complete process of this threat.

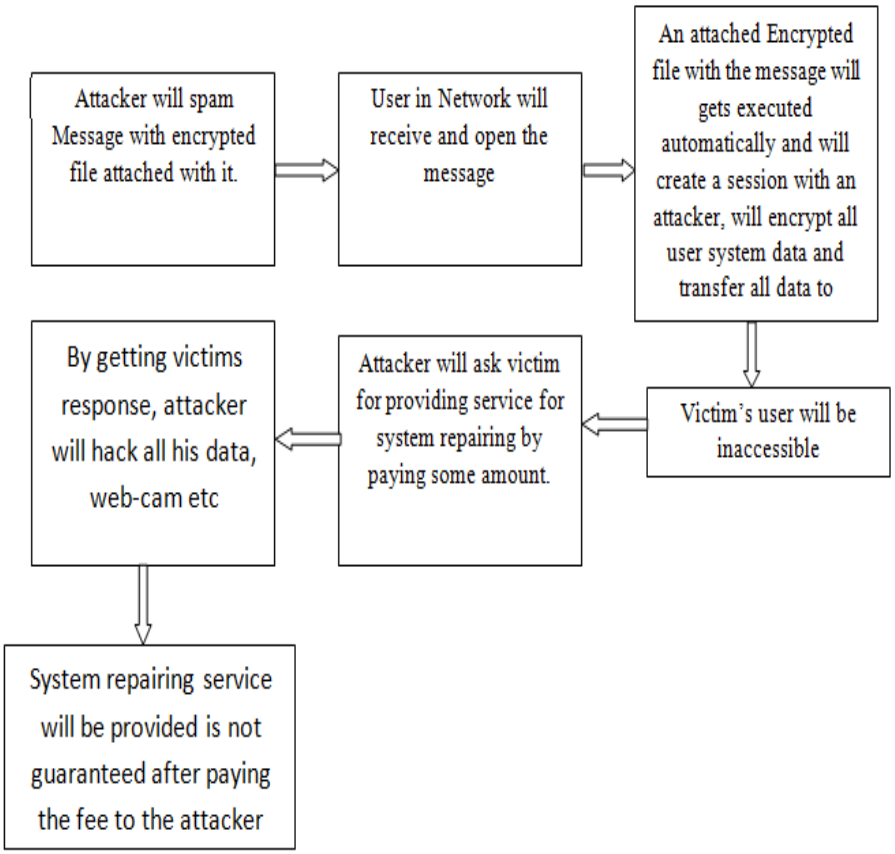

Figure 2. Processing of Threat in Infrastructure

As shown in figure 2. this threat will work in following step.

Step-1) Attacker will transmit spam message to network with an attached file.

Step-2) User in network when receives and open the message an attached file will automatically get executed and will encrypt all data of victim's machine and also create a temporary session in an attacker system.

Step-3) Then attacker will ask victim to provide them a system repairing service with a some servicing fees.

Step-4) As soon as the victim's will respond to attacker's request, his system's data will be transferred to attacker system.

Step-5) Also it is not guaranteed that the attacker will decrypt victim's system data after giving him service charges for sharing decryption keys.

Here in the above system a threat is called as external as well as internal threat where the system is hacked completely and victim has to pay ransom amount too for repairing the system. This threat can be prevented by applying our proposed technique name AdvWEBStuxCRY" which can be implemented using Artificial Intelligence. This technique will use AI method which will work in three different phases i.e. (1) It will prevent the attacker to transmit any spam messages by thrown by the attacker in the network. (2) if the message is received by a victim's machine in the network it will not be opened if clicked by the victim's machine user (3) Its attachment will not get executed even if the message is

ISSN: 2005-4262 IJGDC

opened in the victim's machine. we had named our proposed techniques as "AdvWEBStuxCRY" Technique based on AI methodology.

4. CONCLUSION

In this recent era so many advancements has be explored in web-world. Everybody is using web connection even for communicating while residing or sitting in same couch. Social media is most vulnerable media for sharing vey personal information that can be misused by cyber-criminal for any illegal activities. With these advancement there is a lots threats is also affecting the life of web world user till the extent of their life or death. To prevent this threat we are proposing our research idea which will be used to prevent external as well as internal threat to protect user system data from being hacked by any cyber criminal.

References

[1]. Isern, G. Internet Security Attacks at the Basic Levels ACM SIGOPS Operating Systems Review, 32(2):4–15,2002.

[2]. Frantzen, M. A framework for understanding vulnerabilities in firewalls using a dataflow model of firewall internals, Computers and Security, vol. 20, no. 3, pp., May 2001.

[3]. Householder, A, January 2002. Security & Privacy: "Computer Attack Trends Challenge Internet Security."IEEE Computer Society.

[4]. Howard, J and Longstaff, T. A Common Language for Computer Security Incidents Technical report,Sandia National Laboratories, 1998.

[5]. H. Singh and Geeta, "Cyber Crime – A Threat to Persons, Property, Government, and Societies", *Int. J. of Adv. Research in Comp. Science and Software Engineering*, India, vol. 3, No. 5, pp. 997-1002, May 2013.

[6]. Y. Joshi and A. Singh, "A Study on Cyber Crime and Security Scenario in INDIA", *Int. J. of Engineering and Management Research*, India, vol. 3, No. 3, pp. 13-18, June 2013.

[7].M.Feily,A.Shaherestani,S.Ramadass,Asurveyofbotnetandbotnetdetection,in:SECURWARE2009,pp.268–273

[8].S.Egelman,J.King,R.C.Miller,N.Ragouzis,E.Shehan,Securityuserstudies:methodologiesandbestpractices,in:CHI2007,http://dx.doi.org/10.1145/1240866.1241089

[9].TheCERTguidetoinsiderthreats:Howtoprevent,detect,andrespondtotheftofcriticalinformation,sabotage,andfraud,www.cert.org/archive/pdf/insidercross051105.pdf.

[10]. Regarding the possible ways of infecting a computer system by spyware, see: The spying game: how spyware threatens
corporate security, Sophos white paper, 2005, available

[11]. Hall, J. L (2015, April 20). The NSA's Split-Key Encryption Proposal is Not Serious. *Center for Democracy and Technology*. Retrieved on 12th June 2015 from

ISSN: 2005-4262 IJGDC

[12]. Huber, M., Mulazzani, M., Leithner, M., Schrittwieser, S., Wondracek, G., & Weippl, E.(2011). Social snapshots: digital forensics for online social networks. Paper presented at *Annual Computer Security Applications Conference – ACSAC 2011*, Orlando, Florida

[13].https://www.ennia.com/en/preventionshop/prevention-tips/cybercrime-prevention-tips/

[14]. Goodman, M. D., & Brenner, S. W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*, *10*(2), 139-223.

[15]. Grabosky, P. (2007). Requirements of prosecution services to deal with cyber crime. *Crime, Law and Social Change*, *47*, 201-223.

[16]. Graham, J., Howard, R., & Olson, R. (Eds.) (2011). *Cyber Security Essentials*. Boca Raton: Taylor and Francis Group.

[17]. Hall, J. L (2015, April 20). The NSA's Split-Key Encryption Proposal is Not Serious. *Center for Democracy and Technology*. Retrieved on 12th June 2015.

[18]. Regarding the related challenges, see: *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

ISSN: 2005-4262 IJGDC