American Journal of
Electronics & Communication

Cyber Security and Management

Sanjima Pal[1], Niharika Das[1], Abantika Sarkar[1], Nasrin Begam[1], Lagnadeep Bhowmik [1], Prof. DR. Sudipta Bau Pal [2*]

[1]Department of Computer Science and Engineering

University of Engineering and Management, Kolkata

Kolkata, West Bengal, India

[2]Department of Computer Science Technology and Information Technology Engineering

University of Engineering and Management, Kolkata

Kolkata, West Bengal, India

palsanjima@gmail.com, niharikabnk@gmail.com, abantikasarkar2002@gmail.com, nasrinbegam2011@gmail.com, lagnadip41@gmail.com, sudipta_basu68@yahoo.co.in

***Corresponding Author: sudipta_basu68@yahoo.com**

Abstract

1.To make a secure cyber ecosystem in India, generate an ample amount of trust in IT systems and transactions in cyberspace and thereby enhance the adoption of IT in all sectors of the economy.

2. To create a convincing framework for developing security policies and enabling actions to abidance to global security standards.

3) To build up the Regulatory framework to ensure a Secure Cyberspace ecosystem.

4) To enhance and create National and Sectoral level mechanisms to obtain strategic policy regarding threats to ICT infrastructure.

5) To enhance the protection of the Nation's critical information infrastructure by operating a National Critical Information Infrastructure Protection Centre and mandating

security practices related to the design, accession, evolution, use and operation of information resources.

6) For the growth of suitable indigenous security technologies, solution-oriented research, proof of concept, pilot development, transition, diffusion.

7) To develop the range of the integrity of ICT products and services by establishing infrastructure for testing & validating the security of such products.

8) Create a workspace for 500,000 professionals skilled in cyber security in India within 5years

9) To provide monetary benefits to businesses to adopt standard security practices.

10) To enable security of information while during the process, storage & transit to safeguard the privacy of citizen's data and for reducing financial losses due to cybercrime.

11) To create adequate safety, investigation and prosecution of cybercrime and development of law enforcement capabilities through appropriate legislative intervention.

KEYWORDS: Cyber-Security, Cyber-Threat, Client-Server Model, Cloud Computing

II. Introduction

Cyber Security or information technology security is the collection technique of protecting devices, networks, programs, and data from unauthorized access targeting the exploitation of systems.

Hackers or cyber criminals target customers' personal information like- names, addresses, national identification numbers, credit card details, unique codes- and then give these records to underground digital marketplaces-holders instead of a large amount of money.

Security system complexity, created by contrasting technologies and a team of in-house expertise, can amplify these costs. But organizations with a comprehensive cyber security strategy, controlled by best practices and self-regulating using developed analytics, Artificial Intelligence and Machine Learning (AIML), can fight cyber threats more effectively and cut down the lifecycle and impact of violation when they appear.

III. LITERATURE SURVEY

The internet was born around 1960 "s where its access was limited to few scientists, researchers and the defense only. Internet user base have evolved experimentally. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure. Around 1980's the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called virus. Till then the effect was not so widespread because internet was only combined to defense setups, large international companies and research communities. In 1996, when internet was launched for the public, it immediately became popular among the masses and they slowly became dependent on it to an extent that it has changed their lifestyle. The GUIs were written so well that the user doesn't have to bother how the internet was functioning. They have to simply make few click over the hyper links or type the desired information at the desired place without bothering where this data is stored and how it is sent over the internet or wither the data can accessed by another person who is connoted to the internet or wither the data packet sent over the internet can be snooped and tempered. The focus of the computer crime shifted from merely damaging the computer or destroying or manipulating data for personal benefit to financial crime. These computer attacks are increasing at a rapid passé. Every second around 25 computers became victim to cyber attack and around 800 million individuals are affected by it till 2013. CERT-India has reported around 308371 Indian websites to be hacked between 2011-2013. It is also estimated that around $160 million are lost per year due to cyber crime. This figure is very conservative as most of the cases are never reported. According to the 2013-14 report of the standing committee on Information Technology to the 15th Look Sabah by ministry of communication and information technology, India is a third largest number do Internet users throughout the world with an estimated 100 million internet users as on June, 2011 and the numbers are growing rapidly. There are around 22 million broadband connections in India till date operated by around 134 major Internet Service Providers (ISPs). Before discussing the matter further, let us know what the cyber crime is? The term cyber crime is used to describe a unlawful activity in which computer or computing devices such as smart phones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity. It is often 16 committed by the people of destructive and criminal mindset either for revenge, greed or adventure.

1.2.1 Classification of Cyber Crimes The cyber criminal could be internal or external to the organization facing the cyber attack. Based on this fact, the cyber crime could be categorized into two types:

- Insider Attack: An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparatively easy for an insider to perform a cyber attack as he is well aware of the policies, processes, IT architecture and weakness of the security system. Moreover, the attacker has an access to the network. Therefore it is comparatively easy for an insider attacker to steel sensitive information, crash the network, etc. In most of the cases the reason for insider attack is when an employee is fired or assigned new roles in an organization, and the role is not reflected in the IT policies. This opens a variability window for the attacker. The insider attack could be prevented by planning and installing internal intrusion detection systems (IDS) in the organization.

- External Attack: When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information.Anexpreicend network/security administrator keeps regual eye on the log generated by the firewalls as extertnal attacks can be traced out by carefully analysinig these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks. The cyber attacks can also be classified as structure attacks and unstructured attacks based on the level of maturity of the attacker. Some of the authors have classified these attacks as a form of external attacks but there is precedence of the cases when a structured attack was performed by an internal employee. This happens in the case when the competitor company wants the future strategy of an organization on certain points. The attacker may strategically gain access to the company as an employee and access the required information. 17

- Unstructured attacks: These attacks are generally performed by amatures who don "t have any predefined motives to perform the cyber attack. Usually these amatures try to test a tool readily available over the internet on the network of a random company.

- Structure Attack: These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind. They have access to sophisticated tools and technologies to gain access to other networks without being noticed by their Intrusion Detection Systems(IDSs). Moreover, these attacker have the necessary expertise to develop or modify the existing tools to satisfy their purpose. These types of attacks are usually performed by professional criminals, by a country on other rival countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc. Cyber crimes have turned out to be a low-investment, low-risk business with huge returns. Now-a-days these structured crimes are performed are highly organized. There is a perfect hierarchical organizational setup like formal organizations and some of them have reached a level in technical capabilities at par with those of developed Nation. They are targeting large financial organizations, defence and nuclear establishments and they are also into online drugs trading.

The role of all the people in the hierarchy remain changing and it is based on the oppourtinity. If a hacker who have hacked sesetive data from an organization may use it for financially exploiting the organization himself. In case, the hacker himself have the technical expertise for it, he will do it himself, otherwise he may find a buyer who is intrested in that data and have the technical expertize. There are some cyber criminals offers on-demand and service. The person, organization or a country may contact these cyber criminals for hacking an organization to gain access to some sensetivedata , or create massive denial-of –service attack on their compititors. Based on the demand of the customer the hackers write malware, virus, etc to suit their requirements. An organizaiton effected by a cyber attack, not only faces finincial loss, but its repuration is also adversly affected, and the compitititor organization will definatly benefited by it. 1.2.2 Reasons for Commission of Cyber Crimes There are many reasons which act as a catalyst in the growth of cyber crime.

Some of the prominent reasons are:

a. Money: People are motivated towards committing cyber crime is to make quick and easy money.

b. Revenge: Some people try to take revenge with other person/organization/society/ caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.

c. Fun: The amateur docyber crime for fun. They just want to test the latest tool they have encountered.

d. Recognition: It is considered to bepride if someone hack the highly secured networks like defense sites or networks.

e. Anonymity- Many time the anonymity that a cyber space provide motivates the person to commit cyber crime as it is much easy to commit a cyber crime over the cyber space and remain anonymous as compared to real world. It is much easier to get away with criminal activity in a cyber world than in the real world. There is a strong sense of anonymity than can draw otherwise respectable citizens to abandon their ethics in pursuit personal gain.

f. Cyber Espionage: At times the government itself is involved in cyber trespassing to keep eye on other person/network/country. The reason could be politically, economically socially motivated".

IV. PROBLEM STATEMENT

In the present-day Cyber crime is one of the burning problems of the society. So, the cyber security needs more development to stop the spread of such crimes. Basically the hackers are targeting the client-server model of big organizations, various kinds of public as well as private sector, reputed clubs and their members. Clients will be telling the servers their problems and requirements and the servers will do their best to satisfy their client's needs. But the problem is, the hackers and cyber criminals creates disruption between the communication of client and server. In the client-server model, an interruption free communication is much needed. But the cyber crime creates a problem there and the reputation as well as the finance department of that particular organization faces a huge loss. So, a strong cyber security model is much needed to protect the communication of a client-server model.

V. Proposed solution

A proposed solution is an important communication tool because it examines an issue from multiple angles. Therefore, nowadays cyber threats are constantly evolving. The most effective ways to protect your organization against cyber attacks is to adapt a risk based approach to cyber security like client server management system, where you regularly review your risks and whether your current measures are appropriate.

Therefore here is some proposed solution to protect cyber security model which is client server model.

1. Centralized system with all data in a single place. This is especially beneficial for the network administrator since they have the full control over management and administration. Whatever the problem that occurs in that entire network can be solved in one place. And also due to this, the work of updating resources and data has become way easier.

2. Cost efficient requires place maintenance cost and data recovery is possible. Since all the files are stored in the central server, it is rather easy to manage files. In client server network has the best management to track and find records of required files. So it is cost efficient.

3. The capacity of the client and servers can be changed separately.

4. Irrespective of the location of the platform every client is provided with the opportunity to log into the system. By this way all the employees will be able to access their corporate information without needing to use a terminal mode or a processor.

5. In client server network, the data is well protected due to centralize architecture. It can be in force with access controls such that only authorized user are granted access. One such method is imposing credentials like- user name and password. Moreover , if the data where to be lost the files can be easily recovered from a single backup.

VI. Result

This project belongs to client-server model.

The Client-server model is a application structure that partitions task between the resources, called servers, and clients. In the client-server infrastructure, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and delivers the message requested back to the client. Clients do not share any of their resources. Examples of Client-Server Model are Email, World Wide Web, etc.

Working of Client-Server Model:

We are going to take a look into the Client- Server model that how the internet works via, web browsers. This report will help us in having solid information of the web and help in working with web technologies with ease.

Client: It means an organization using a particular service.
Similarly in the digital world a client is a computer (Host) i.e., capable of receiving information or using a particular service from the service providers (Servers).

Servers: It means a person or medium that serves something. In this digital world a Server is a remote computer which provides information (data) or access to particular services.

So, it's basically the Client requesting something and the Server serving it as long as it's present in the database.

Interaction of client and server side:

There are socket programs to connect with client and server side. Socket programming is a method to connect two sockets on a network to communicate with each other. One socket listens to a particular port at an IP, while other socket reaches out to the other to form a connection.

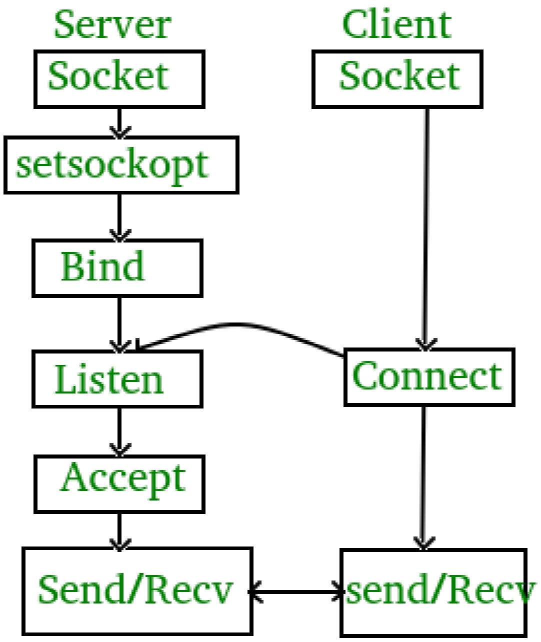

Figure: socket interaction with client and server part.

Server creates the listener socket while client reaches out to the server.

Input:

Client

```
Printf("Hello message sent");
```

Server

```
Printf("Hello message sent");
```

Output:

```
Client- hello message sent

Hello from server

Server- Hello from client

Hello message sent
```

VII. Conclusion

Here the entire network is composed of client-server model which is controlled by a centralized server. A web-server has the capability to perform large operations like network management. Using the correct method, they can be implemented on various types of resources such as electrical gadgets etc.

Many corporations, now-a-days, work across the countries utilizes Client-Server Model which helps them to connect with others using a centralized database.

At present, we witness the client-server model extend even further to the network. Essentially, the network is just a larger more inter-connected server that you rent from a network provider. The client is still making requests and receiving files from the server in much easy way. The client server model is so effective at maintaining consistency across large collections of clients. Its' hard to imagine IT best practices switching to another alternatives.

VIII. Future of cyber security:-

It is crystal clear that the future of internet and internet user is in the hand of Cyber security. Today we even can't imagine visiting any web page without proper cyber security.-

1. The whole project is done using Dev c++ compiler and in C programming language. If anyone wants to develop this with any other language and in any other compiler, he or she can do so. As example- as the program was written in C language, we had to use many lines to write it. If the program was written in python there was less number of lines.

2. Cloud computing makes it faster, cheaper and easier than ever to put the services online and collect a huge amounts of data. It also protects us from unsecured network.

3. The sates of password allow us to protect the data from an unknown network like now a days, we have to use a password which includes letters, symbols, numbers, and special characters which make the hackers unable to reach out our personal information. So, we need to choose our password wisely.

4. Artificial intelligence approaches both the cyber criminals and cyber security team it is very effective in handling massive amount of data. AI is also being used to learn about new attack patterns in cyber crime.

5. IOT is also being used to make the electrical devices (which we use to make our daily life easier) secured from phishing attack.

REFERENCES

1. Aghajani, G., Ghadimi, N., 2018.Multi-objective energy management in a micro-grid Rep. 4, 218-225.
2. Ahmed Jamal, A., et al., 2021. A review on security analysis of cyber Aghajani,

G.,Ghadimi, N., 2018. Multi-objective energy management in physical systems using machine learning.

3. Akhavan-Hejazi, H., Mohsenian-Rad,H., 2018. Power systems big data analytics:An assessment of paradigm shift barriesrs and prospects.Energy Rep. 4, 91-100
4. AL-Ghamdi,M.l.,2021. Effects of knowledge of cyber security on prevention of attacks .
5. AI Shater, D., et al., 2020. Hydroxamate siderophores:Naturaloccurance,chemicalsynthesis,iron binding affinity and use as Trojan horses against pathogens Eur. J. Med Chem 208,112791.
6. Alghamdi, M.l., 2021. A novel study of preventing the cyber security threats .
7. Alhayani, B., et al., 2021., Best ways computation intelligent of face cyber attacks.
8. Alibasic ,A., et al., 2016. Cybersecurity for smart cities: A brief review .In:International Workshop on Data Analytics for Renewable Energy Integration.Springer.
9. Alkatheiri,M.S., Chaudhury ,S.H., Alqarni, M..A., 2021. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications .Sustain. Energy Technol access .45,101219
10. Alzubaidi,A., 2021. Cybercrime awareness among Saudi nationals:Dataset. Data Brief 36, 106965.
11. Amir, M., Givargis T., 2020 pareto optimal design space exploration of cyber-physical systems.Internet Things 12, 100308.
12. Arend, I., et al., 2021., 2020 . Passive and not active-risk tendencies predict cybber security behaviour .Comput.Secur.97, 101964.
13. Aziz, A.A., Amatul , Z., 2019 . Developing Trozan horses to induce ,diagnose and suppress Alzhemir's pathology . Phaemacol Res. 149, 104471.
14. Baig Z.A., et al., 2017 Future challenges for smart cities :Cyber-security and digital forensics digit .Investing .22, 3-13.
15. Beechey ,M. Kyeiakopolous , K.G., Lambotharon, S., 2021. Evidential classification and feature selection for cyber-threat hunting.Known-based Syst .226,107120
16. Bullock, J,A., Haddow, G.D., Copolla D.P., 2021, cybersecurity and critical infrastructure protection .In :Bullock , J.A., Haddow, G.D., Coppola , D.P.(Eds), introduction to Homeland Security ,sixth ed. Butterworth-Heinimannpp. 425-497 (chapter 8).
17. Cao, Y., et al., 2019. A topology-aware access control model for collaborative cyber-physical spaces:Specification verification Comput. Secur. 87. 101478.
18. Cao. J al., 2021. Hybrid- triggered -based security controller for net work control system un der multiple cyber attacks. Inform Sci. 548, 69-84.
19. Azhraf, J., et al., 2021. IoTBoT-IDS:A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities .Sustainable Cities Soc. 72, 103041.