© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 13 Issue: 02 | April - June 2022
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewe

USE OF CRYPTOGRAPHY IN SECURITY ENHANCEMENT FOR PREVENTING CYBER CRIME

Shivneet Singh
Email id :- redhu.shivneet3@gmail.com

ABSTRACT: The effects of cybercrime have been outlined in this research. The Internet-facilitated criminal activity. Cybercrime is the term used to describe these forms of wrongdoings. Controls for network security have been implemented to prevent hackers from gaining access. The usage of VPNs and other forms of encryption technology are used here. To prevent hackers from gaining access to networks, this strategy relies heavily on VPNs. Using a virtual private network (VPN) enables users to have direct access to network resources. It's possible it exists on a public network like the internet. We can combat cybercrime by combining cryptography and steganography. Those who lack familiarity with cybercrime and its consequences might benefit from reading this material. The ability to spot patterns of cybercrime would be very useful. Understanding the efficacy of laws against cybercrime is also determined.

KEYWORD: Cyber crime, Steganography, Cryptography, Phishing, Cyber Terrorism, Spamming, Hacking, fraud, Visual cryptography, Encryption, Decryption, upload, download

[1]INTRODUCTION

In the realm of cybercrime, electronic means of communication are used. Child pornography, graphic design, and online fraud transactions are all part of this category of illicit behavior, as are attacks on data systems and theft of products over the internet. Likewise, deployments in criminal online activity are a reality. Viruses, worms, and other forms of malicious software, as well as phishing and other email scams, are all examples of illegal acts. To prevent hackers from gaining access to networks, this strategy relies heavily on VPNs. Using a virtual private network (VPN) enables users to have direct access to network resources. Telecommunication network assaults, theft of telecommunication services, and fraudulent data manipulation by computer users are all on the rise.

[2] OBJECTIVES

There are several objectives that are put forward in the research work. Such objectives are listed below:

- To identify the problems and challenges in cyber sector due to crime.
- To identify the trends of crime in cyber sector.

- Highlight present state of response to cyber offence in India;
- Highlight the level of main concern cyber crime for law enforcement association.
- To know the effectiveness of law regarding cyber crime.
- Set the recommendations for additional knowledge and feasible enhancement in state of give the answer to cyber crime in India.

[3]PROBLEM STATEMENT

Indian cyber crime: current difficulties and technological obstacles for investigation and prevention.

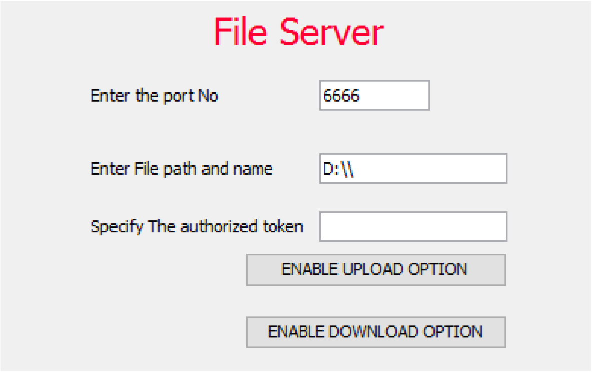
Numerous subgenres of hackers and crackers are to blame for today's widespread cybercrime. Anyone with the ability to breach a system might be considered a black hat. He logged in without the owner's permission. Particularly, it was done with ill will. Depending on local regulations, such actions might be prohibited. It's often referred to as "cracking" software. In the hacking world, a Grey Hat is a seasoned pro. At times he even acts legitimately in his character. However, there are a few of instances when he engages in criminal behavior. Grey hat hackers combine white and black hat techniques. Typically, they won't launch an assault for the sake of scoring a personal victory. Online criminals, often known as hackers, commit crimes using the Internet as their medium. Internet-based abduction includes incidents like those described above as well as fraud and cyberterrorism. They use computers to carry out these crimes.

[4] IMPLEMENTATION WORK

In this research, a server application and client application have been developed by us. These applications have been created in Net bean IDE. These are indicated by the below given figure:

(a)Server Side Implementation

In this research, a server application and client application have been developed by us. These applications have been created in Net bean IDE. These are indicated by the below given figure:



File Server

Enter the port No: 6666

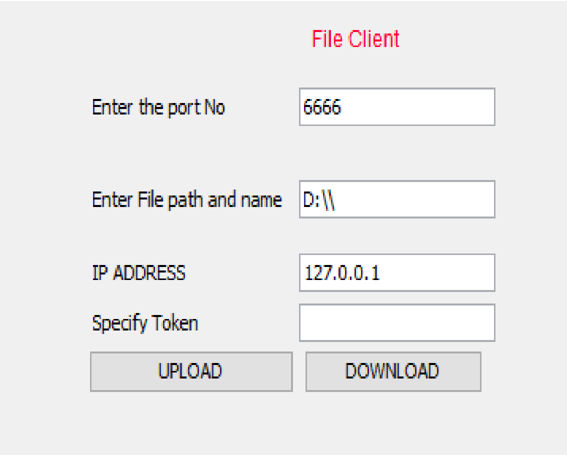
Enter File path and name: D:\\

Specify The authorized token:

Fig: 1 The Design View of Server Side Application

(b)Client side implementation

The below given is the design view for file client in to upload and download the information. Port no, file path are specified here. Here the IP address of server and token (to encode data) are also specified.



File Client

Enter the port No: 6666

Enter File path and name: D:\\

IP ADDRESS: 127.0.0.1

Specify Token:

Fig: 2 Code to implement UPLOAD on client side

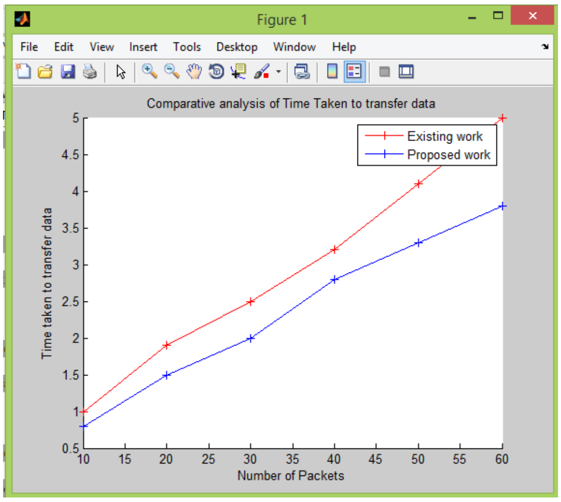


Fig 3 Comparison of time taken to transfer packet

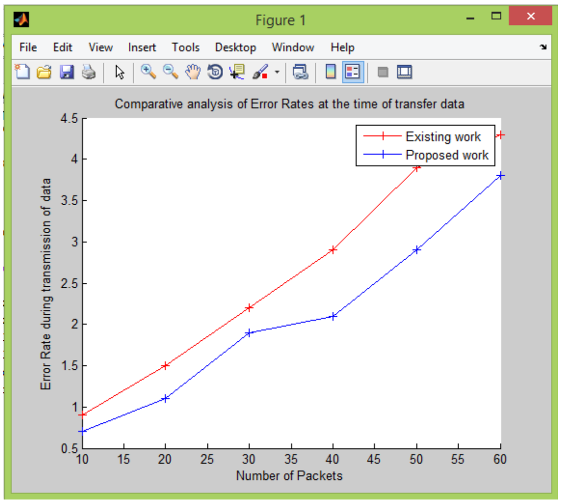


Fig 4 Comparison of error rates at the time of transfer data

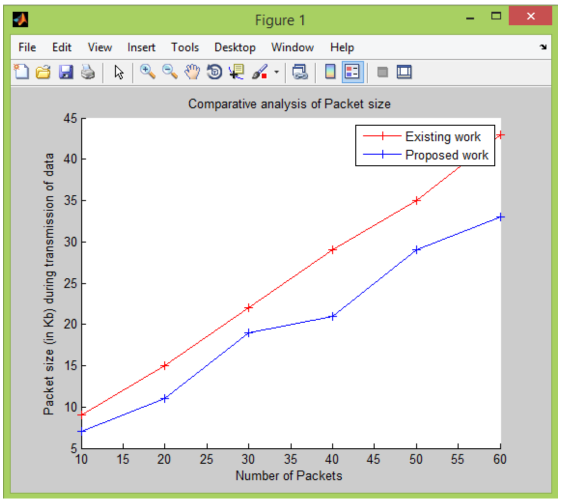


Fig 5 Comparison of packet size

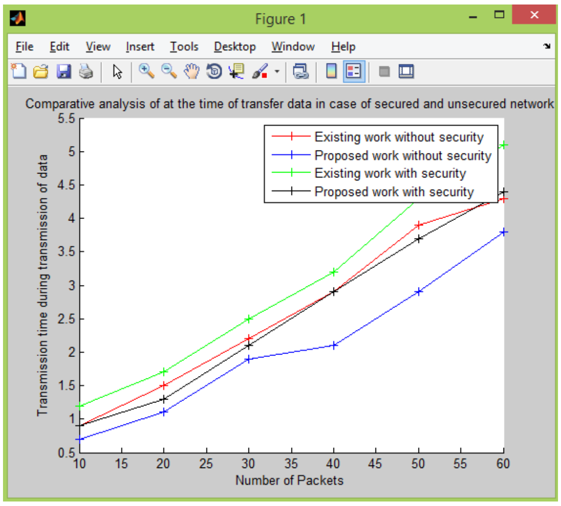


Fig 6 Comparative analysis of transmission time taking by traditional and proposed work

[5]CONCLUSION

Dynamic tainting has been used to determine reliable data sources and to label data obtained from these sources. Keywords and operators in SQL are a good illustration. We find that by using this strategy, we may limit the number of false negatives that arise from using data from unreliable sources without first thoroughly investigating its veracity. In rare instances, a false positive may occur. The delay between packet transmission and typical testing methods. Testing processing latency during packet sharing was also taken into account throughout this study's analysis. We also do research into the testing delay in queueing of network packets in a cloud setting. It has been resolved by using dual steganography to overcome the security issues. Dual Steganography has been characterized as the blend of Cryptography and Steganography.

[6]FUTURE SCOPE

The research objective is the avoidance of cyber crime with the use of cyber laws as well as cyber security techniques. The cyber security techniques categorizes correctly and sufficiently. These are capable to detect the doubtful URLS. These capture the malware samples. The phishing websites are also captured with the use of clustering mechanisms. Nowadays the security tests are efficient to capture the web application susceptibilities with the use of balanced concept.

References

[1] Abhishek Kumar Bharti, "Detection of Session Hijacking and IP Spoofing Using Sensor Nodes and Cryptography"IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p-ISSN: 2278-8727 volume 13, Issue 2 (Jul. -Aug. 2013), PP 66-73

[2].Hani Alshamrani, "Internet Protocol Security (IPSec) Mechanisms", International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014, pp. 85-87.

[3].ChanderDiwakar, Sandeep Kumar, Amit Chaudhary, "SECURITY THREATS IN PEER TO PEER NETWORKS", Journal of Global Research in Computer

Science, Volume 2, No. 4, April 2011, pp. 81-84.

[4]. HaroonShakiratOluwatosin, "Client-Server Model", Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 1, Feb. 2014, pp. 67-71.

[5]. Ms. Jasmin Bhambure, Ms. DhanashriChavan, Ms. Pallavi Band, Mrs.LakshmiMadhuri, "Secure Authentication Protocol in Client – Server Application using Visual Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014, pp. 556-560.

[6]. Mohan V. Pawar, Anuradha J, "Security of network and Types of Attacks in Network", International Conference on Intelligent Computing, Communication & Convergence, 2015, pp. 503 – 506.

[7]. MANJIRI N. MULEY, "ANALYSIS FOR EXPLORING THE SCOPE OF NETWORK SECURITY TECHNIQUES IN DIFFERENT ERA: A STUDY", International Journal of Advanced Computational Engineering and Networking, Volume-3, Issue-12, Dec.-2015, pp. 33-36.

[8]. Rupam, AtulVerma, Ankita Singh, "An Approach to Detect Packets Using Packet Sniffing, International Journal of Computer Science & Engineering Survey (IJCSES) ,Vol.4, No.3, June 2013, pp.21-33.

[9]. Sharmin Rashid, SubhraProsun Paul, "Proposed Methods of IP Spoofing Detection & Prevention, International", Journal of Science & Research (IJSR), Volume 2, Issue 8, August 2013, pp.438-444.

[10]. MukeshBarapatre, Prof. Vikrant Chole, Prof. L. Patil, "A Review on Spoofing Attack Detection in Wireless Adhoc Network", International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 6, November – December 2013, pp.192-195.

[11]. Amandeep Kaur, Dr. Amardeep Singh, "A Review on Security Attacks in Mobile Ad-hoc Networks", International Journal of Science & Research, Volume 3 Issue 5, May 2014, pp.1295-1299.

[12]. Md. Waliullah, Diane Gan, "Wireless LAN Security Threats & Vulnerabilities", International Journal of Advanced Computer Science & Applications, Vol. 5, No. 1, 2014, pp.176-183.

[13]. P. Kiruthika Devi, Dr. R. Manavalan "Spoofing attack detection & localization in wireless sensor network", International Journal of Computer Science & Engineering Technology, Vol. 5, No. 09, Sep 2014, pp.877-886.

[14]. BarleenShinh, Manwinder Singh, "A Review Paper on Collaborative Black Hole Attack in MANET", International Journal of Engineering & Computer Science, Volume 3, Issue 12, December 2014, pp. 9547-9551.

[15]. Ms. VidyaVijayan, Ms. Josna P Joy, Mrs. Suchithra M S, "A Review on Password Cracking Strategies", international Journal of Research in Computer & Communication Technology, 2014, pp.8-15.