A RESEARCH ON A COMPARATIVE STUDY OF CYBER LAW IN AVOIDANCE OF CYBER-CRIME TOWARDS CYBER SECURITY DEVELOPMENT

Mohammad Istekhar
Research Scholar
Department of Computer Science
Sunrise University
alam2611985@gmail.com

Dr. Amit Jain
Research Guide
Department of Computer Science
Sunrise University

Abstract:-

Cybercrime refers to criminal activities that are carried out through the internet or other digital communication networks. In India, cybercrime has become a major concern in recent years, with an increasing number of people using digital devices and the internet for various purposes. To address the issue of cybercrime, the Indian government has enacted various laws and regulations. The primary legislation in this regard is the Information Technology Act, 2000, which was amended in 2008 to provide more teeth to the law in tackling cybercrime. Other relevant laws include the Indian Penal Code, the Criminal Procedure Code, and the Indian Evidence Act. Some of the common types of cybercrime in India include hacking, phishing, identity theft, cyber stalking, and online fraud. To combat these crimes, the government has set up various agencies such as the Cyber Crime Investigation Cell, the Cyber Appellate Tribunal, and the National Cyber Security Coordinator. The penalties for cybercrime in India can range from fines to imprisonment, depending on the severity of the crime. For example, hacking can result in imprisonment for up to three years and a fine of up to five lakh rupees, while cyber stalking can result in imprisonment for up to three years and a fine. Overall, the Indian government has taken significant steps to address the issue of cybercrime, and it is important for individuals and organizations to be aware of the laws and regulations in place to protect themselves from cyber threats.

Keywords:-Cyber law , Cyber crime, cyber security

INTRODUCTION

RESEARCH MOTIVATION

The internet plays a crucial role in human existence in the 21st century, especially in terms of making life simpler in terms of making better use of time and increasing the overall execution factor. In particular, this is the case when it comes to enhancing the overall execution factor. As we go forward into the present day, it has developed into the cornerstone upon which the existence of humans is constructed. The internet has made it possible for governments, organizations, and people all over the globe to become more reliant on the many facilities and services that it provides.

The internet has opened the door to a multitude of new opportunities, including real-time communications, electronic money transactions, the flow of information, access to government services, and a myriad of other possibilities that have greatly changed the contemporary day. The pervasiveness of people's reliance on the internet is common knowledge at this point. On the other hand, there is another side to the tale, and that side is the growth in online crime that has been produced by the greater use of the internet. This rise in online crime has been generated by the growing use of the internet. In this context, cyber security plays an important role in detecting the repercussions of such risks and devising solutions to fulfill those implications.

PROBLEM STATEMENT

The task of digitizing data is challenging, and as a direct result of this, the degree to which cyber security can be regulated has arisen as a significant area of concern.

This is a problem since it might have severe implications. In addition, with the introduction of e-commerce, a major rise in the usage of credit cards for financial transactions conducted online has occurred. It's possible that this was one of the contributing reasons that contributed to the significant rise in the number of cases of credit card fraud. The credit card business has a significant and pervasive issue in the form of fraud, making it one of the most significant and important ethical problems.

The act of cyberstalking has become increasingly common and is now being recognized as a criminal violation as a result of developments in technology and an increase in the number of people who have access to and are able to utilize technology. As a result of these developments, the number of people who are able to utilize technology has also increased.

In a nutshell, the problem may be segmented into the following areas for easier comprehension:

• Raise public awareness about cybercrime

• Reduce the amount of money lost online due to criminal activity Cyber losses are a more difficult problem.

• Theft Can Be Identified

• Detection of fraudulent use of credit cards

• Detection of fraudulent use of credit cards

• Protection against phishing attacks

• Decrease in the incidence of cybers talking

SCOPE

This research focuses on the analysis and design of cyber security technologies, as well as examining how businesses manage their cyber security ambitions, risks, and threats in the digital realm. This is essential due to the very high number of firms who are now addressing concerns around cyber security.

In addition, the focus is on cyber security rather than the information security field in general, which is a somewhat bigger domain. Phishing, cybers talking, cybe rbullying, and credit card fraud are just a few examples of the kind of issues that may be addressed by the use of cyber security measures.

ORIGIN OF INTERNET

ARPANET, the world's first high-speed, continental computer network, was built by the Defense Advanced Research Projects Agency (DARPA). In most people's minds, ARPANET may be thought of as the Internet's predecessor. Developed with assistance from the United States of America Larry Roberts was the one who, in the year 1964, was the first person to have the notion of developing a network that would be comparable to the one that we have today.

This network would be decentralized, which means that there would not be a single central computer that acts as the hub of the network. Instead, the network would be comprised of several computers working in conjunction with one another. In the event of a nuclear war, a computer like this one would be very susceptible to damage. In its place, there would be a number of unique components, each of which would carry out its tasks independently of the others.

CYBERSPACE

In 1990, the public was given its first glimpse of what would become known as the World Wide Web. Since that time, the vast majority of communities has embraced digital technology and are now linked to what we refer to as cyberspace.

Since 1991, a sizeable number of people have joined, and cyberspace has evolved the capability to influence all elements of the civilized society as a result.

The word "cyberspace" does not yet have a meaning that is widely recognized since it involves everything from software to hardware to the Internet to information to links to servers to personal computers and even relationships between people, governments, organizations, and society.

CYBERCRIME AND EXPLOIT

The concept of cybercrime as an everyday kind of criminal conduct is still relatively new to the community at large. In this context, the term "cybercrime" refers to any illegal behavior that takes place on or through the medium of a computer or the internet or any other kind of technology that is specifically named in the Information Technology Act.

This definition encompasses a wide range of activities, including fraud, identity theft, and the distribution of malware. Cybercrime is the most pervasive kind of organized crime in modern India, and it plays a staggering role in the country's economy. Not only have criminals been responsible for a significant amount of harm to society and, as a direct consequence, to the government, but those criminals are also able to keep their identities a secret.

Management of Cyber Security Risks

• The threat may take the form of a human, an item, or a different substance altogether, and it poses a persistent danger to an asset. It is anything that will take advantage of the vulnerability, either intentionally or accidentally, in order to cause damage or destruction to an asset.

• Vulnerability may represent a gap or weak spot in our attempts to ensure safety.

• Impact a successful attack can trade off the confidentiality, integrity, and availability of an information and communications technology framework and the data it handles.

• A vulnerability is an imperfection or weakness in an information asset, safety technique, technical design, or control that a risk may exploit purposefully or may be accidentally to break the security system.

The current study is based on both qualitative and quantitative research assessments; they served as the investigation's basis. The researcher had the idea that a survey in the form of a questionnaire might be used to learn more about the many forms of cybercrimes that are prevalent in today's society as well as to evaluate the degree to which people are aware of them. There are a total of one hundred participants in the survey, and they come from all around the city. For the objectives of this investigation, we focused on analyzing responses from participants in the age range of 18 to 35 years old. Hacking, cyberstalking, phishing, malware assaults, email spamming, and viruses are just few of the various forms of cybercrime that may occur on a daily basis. Other sorts of cybercrime include viruses and spam emails.

Table 3.1 Cybercrime List

C1	Hacking
C2	Phishing
C3	Cyber talking
C4	Virus
C5	Email Spam
C6	Online identify Theft

Awareness of Precaution during Cybercrime

• 59% of respondents said they often changed their login information.

• 63 percent of respondents take precautions to safeguard their identity online.

• Forty-two percent of respondents make use of or activate a firewall.

• Thirty percent of respondents utilized antivirus software, while 61 percent shopped on safe websites.

• Approximately forty-three percent of respondents check the links to files before clicking on content from an unidentified source.

• Before publishing anything on social media, 56 percent of respondents check the security settings.

• While accessing public Wi-Fi Hotspots, 52% of respondents maintain a vigilant attitude.

• It is evident that 62 percent of respondents had the same opinion on the uneasy sensation associated with the security of online transactions.

REDUCING IDENTIFIED THEFT

The process of encrypting and decrypting data requires the application of mathematics. You are able to transfer or keep sensitive data over unstable networks by using encryption, which ensures that only the intended receiver may see the data. The field of research known as cryptography focuses on the management of information in the setting of secret or encrypted communication.

The present state of cryptography puts a significant focus on data secrecy, data integrity, authentication, and non-repudiation and there are a number of different elements that may affect information security. This chapter presents a method that is supported by symmetric cryptography and makes use of ASCII values. It is designed to lessen the likelihood of theft being identified.

AVOIDENCE OF CYBER STALKING

When one person persistently threatens or harasses another person online, this behavior may be called cyber stalking and may be unlawful in certain jurisdictions. Cybers talking may take place via a variety of internet channels, including social media, instant messaging, email, chat rooms, and clients, amongst others. It is also possible for it to occur concurrently with the more traditional form of stalking, in which the offender engages in various forms of offline harassment directed against the victim.

PREVENTION AGAINST PHISHING ATTACK

In today's increasingly interconnected world, the threat posed by phishing is only going to increase. An attacker often conducts a phishing attack on a mobile phone device by sending an SMS message that contains a link to phishing web sites or applications that, if wanted, solicit credentials. Attacks might be launched using email messages that have accumulated in the browser of a mobile device.

User interfaces are necessary for the limited screens seen in mobile phone devices. In particular, for communication with mobile operating systems and browsers, secure apps or websites are essential. A client has no way of knowing for certain which mobile application or website she is using at any one time. The end user runs the risk of mistaking malicious software for a trustworthy one as a result of this.

CONCLUSION

People have a tendency to access links on their mobile phones without first having a complete comprehension of the URLs of those links, and they also pay inadequate attention to any potential phishing efforts that may be taking place. Another issue that usually impacts businesses that deal with finances is when customers download and install software without realizing that the apps they have installed could not be authentic official versions. This is a common problem. In this chapter, we gathered mobile applications that have user permission and analyzed them using a Nave Bayesian technique. This kind of machine learning technology allows the system to differentiate between legal and malicious applications, which is an important security feature. Our technique distinguishes between various keyloggers based only on their behaviors, which are characteristics that are typical of all keyloggers. This method does not rely on doing an in-depth examination of the keylogger itself. Memory use, control flow, and resource consumption are all potential candidates for inclusion in the future as a feature vector that might assist in identifying keyloggers.

FUTURE WORK

Today, the term "cyber security" refers to the protection of broader digital networks in addition to the protection of information technology systems inside enterprises. These larger digital networks comprise both cyberspace and the necessary infrastructure that supports it. The growth of information technology and services is heavily impacted by the state of cyber security. Improving the nation's cyber security and safeguarding its important data infrastructures are of the utmost importance for the country's physical protection and economic prosperity. Cyber networks are now essential to every aspect of human effort, including commerce, finance, healthcare, energy, entertainment, communication, and even the protection of the nation's borders. According to the findings of the study, an increasing number of people are worried about their privacy and the disclosure of personal information.

REFERENCES

1. *PwC Survey, "Fighting Economic Crime in the Financial Services Sector", pp. 1-16, 2012.*
2. *T. Ristenpart, E. Tromert, H. Shacham, S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", In Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 192–212, 2009.*
3. *PwC Survey, "US cybercrime: Rising Key findings", 2014.*
4. *Gemalto, "Breach Level Index Annual Report 2014", pp.1-16, 2015.*
5. *R V. Solms, J. V. Niekrek, "From Information Security to Cyber Security", Computers & Security, vol. 38, pp. 97–102, 2013.*
6. *Verizon, "2014 Data Breach Investigations Report", pp. 2-56, 2014.*
7. *E. Byres, J. Lowe, "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", In Proceedings in VDE Kongress, vol. 112, pp. 1–6, 2004.*
8. *Deloitte, "Blurring the lines 2013 TMT Global Security Study", pp. 5- 19, 2013.*
9. *S. R. Chabinsky, "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line", Journal of National Security Law & Policy, vol. 4, pp.27–39, 2010.*
10. *The National Military Strategy for Cyberspace Operations, Chairman of the Joint Chiefs of Staff, Washington, D.C., 2006.*
11. *J. Andress, S. Winterfeld, "Cyber Warfare: Techniques", Tactics and Tools for Security Practitioners, pp. 1-277, Elsevier, 2011.*
12. *M. Barret, D. Bedford, E. Skinner, E. Vergles, "Global Commons Maritime Air Space Cyber", NATO, Norfolk, 2011.*
13. *R. M. Yusof, M. F. Sukimi, S. B. Ismail, Z. B. Othman, "The Cyber Space and Information,*

Communication and Technology: A Tool for Westernization or Orientalism or Both", Journal of Computer Science, pp. 1784-1792, 2011.

14. The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, US Army TRADOC Pamphlet 525-7-8, pp. 1-72, 2010.

15. T. Parfitt, "Georgian Woman cuts off Web Access to Whole of Armenia", The Guardian, 2011.

16. L. Lessig, "The Future of Ideas", The Fate of the Commons in a Connected World, New York: Random House, 2001.

17. S. Kim, S. Seo, I. Lee, "Essential Characteristics of Cyberspace and Analysis of Cyber Educational Institutions", In Proceedings of the 3rd Asia-Pacific International Conference on computational Methods in Engineering (ICOME2009), pp.1-5, 2009.

18. D. S. Reveron, "Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World", Georgetown University Press, vol. 34, issue 1, pp.254-256, 2012.

19. V. K. Gunjan, A. Kumar, S. Avdhanam, "A Survey of Cyber Crime in India", 2013 15th IEEE International Conference on Advanced Computing Technologies (ICACT), pp.1-6, 2013.

20. W. Mazurczyk, T. Holt, K. Szczypiorski, "Guest Editors' Introduction: Special Issue on Cyber Crime", IEEE Transaction on Dependable and Secure Computing, vol.13, pp. 146-147, 2016.