Journal of Science, Computing and Engineering Research (JSCER)
Volume-7, Issue-6, June 2024.
DOI: *https://doi.org/10.46379/jscer.2023.070604*
ISSN: 2708-1079

A Comparative Review Study on Cyber Crime in recent Aspects

Shivaji Kachare

Assistant Professor,venkateshwara College of Engineering, EEE Dept, Kannor, India

Article Information

Received : 02 June 2024
Revised : 06 June 2024
Accepted : 18 June 2024
Published : 22 June 2024

Abstract— Cybercrime is one of major problem that people face now a days and it effects the individual, organizations and even the Government. Cybercrime is basically a crime in which an offence is committed against an individual or group of people and itharms their emails, websites and mobile phones. This paper introduces review on cybercrime in detail

Corresponding Author:
Shivaji Kachare

Keywords: ***Dynamic latch comparator, speed, power consumption, high speed analog to digital converter.***

Citation: Shivaji Kachare "A Comparative Review Study on Cyber Crime in recent Aspects", Journal of Science, Computing and Engineering Research, 7(7), June 2024.

I. INTRODUCTION

The term crime is denoted as an unlawful act which is punishable by a state. Crime is also called as an offense or a criminal offense. According to the authors in, cyber is a prefix used to describe a person, thing or idea as a part of the computer and information age. It involves computer or computer networks. A computer network is basically the collection of communicating nodes that helps in transferring data across. The nodes at any given time could be a computer, the laptop, smart phones etc. Cybercrime encompasses any criminal act dealing with computers and networks. It includes crime conducted through the Internet. The Internet is basically the network of networks used across for communication and sharing of data. Cybercrime also known as the computer crime is the use of an instrument for illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. With the advancement of the Internet technologies like the 2G and 3G, the global village is effectively sharing and communicating vital data(s) across the network

II. RELATED WORKS

Cybercrime encompasses a wide range of crimes including stealing people's identity, fraud and financial crimes pornography, selling contraband items, downloading illegal files etc. Some of the popular and alarming crimes in the cyber world are discussed below:

The criminals of credit card fraud get information from their victims often by impersonating a Government official or people from financial organizations asking for their credit information. The victims fall prey to this without proper inquiries and give away their credit card information to these criminals. Cyber Pornography Pornographic websites which allow downloading of pornographic movies, videos and pictures, on-line pornography magazines (photos, writings etc.), all come under this category. The study made by the UK Home Affairs Committee Report on Computer Pornography (House of Commons, 1994) says that "Computer pornography is a new horror" (House of Commons, 1994:5). Drug Trafficking Drug traffickers contribute a major part of cybercrime to sell narcotics using the latest technologies for encrypting mails. Since there is no personal communication between the buyer and dealer, these exchanges are more comfortable for intimidated people to buy illegal drugs and even other items. Cyber Terrorism Cyber terrorism may include a simple broadcast of information on the Internet about bomb attacks which may happen at a particular time in the future.Cyber terrorists are people who threaten and coerce an individual, an organization or even a government by attacking them through computers and networks for their personal, political or social benefits. Online Gambling On-line gambling offered by thousands of websites that have their servers hosted abroad.

III. BACKGROUND OF STUDY

There are different types of cybercrime today. But the eight most common ones are: Theft in the Services of Telecommunication Individuals and criminal organizations can gain access to the switchboards of an organization's switchboard and obtain the access to their dial-in or dial-out circuits. The criminal is usually asked to pay a fine with a short amount of jail time. Piracy of Telecommunication When the creators of a particular work are not able to gain profit from their own creations, it leads to severe financial loss and a great effect on creative efforts generally.

Laundering E-money and Evasion of Taxes Central bank supervision will be bypassed by the development of the informal banking institutions or the parallel banking systems. There is no separate law for this type of crime committed using computer and a network, but it falls directly under the laws which cover these offenses in general. Illegal Interception of Telecoms Signals The great and fast development in telecommunications allows new opportunities for electronic eavesdropping. The existing laws today, does not prevent one from monitoring a computer radiation from a distance. Fraud in Transfer of Electronic Funds Electronic transfer systems are proliferating, and the same goes with the risks that such type of transactions may be intercepted or diverted. With the usage of electronic fund transfer system, there is no doubt that this system will enhance the risk. Year 2009 showed a hike of about 559.7 million U.S. dollars and later by 2017 the monetary damage grew to 781.84 million U.S. dollar which is certainly alarming

IV. METHODOLOGY

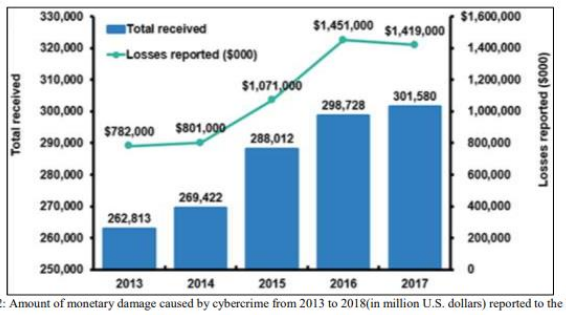


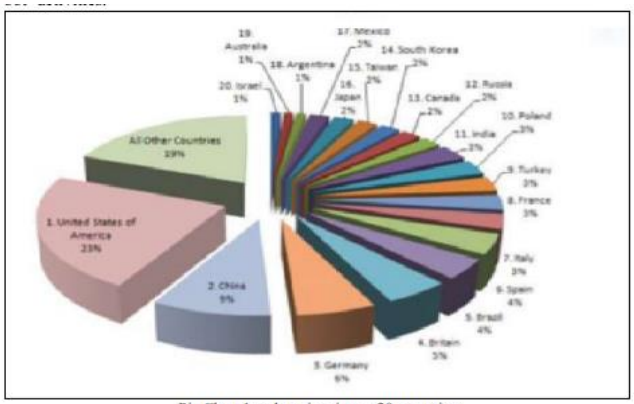
Fig. 2: Amount of monetary damage caused by cybercrime from 2013 to 2018(in million U.S. dollars) reported to the IC3.

Symantec – A famous Security Firm, carried out a detailed study and has been able to find out the top ranked 20 countries that were facing and/or causing most of the activities of cybercrime. The design was made to trick users so that the computer user discloses their personal information or banking account information. In its further investigation, Symantec was successfully able to acquire the data including the number of bot-infected systems. These systems were meticulously controlled by the cybercriminals. The higher rate of cybercrime was found to be in the United States of America. This could be because the country is well facilitated with the broadband connection providing uninterrupted internet connection. Table 1 shows the countries that had been the victims of cybercrimes such as sharing malicious computer activities, spam messages, phishing etc. The table 1 shows, the six factors; 1) Share of malicious computer activity, 2) Malicious code rank, 3) Spam zombies rank, 4) Phishing web site hosts rank, 5) Bot rank and 6) Attack origin, These factors contribute to authenticate its cybercrime ranking as conducted by Symantec security organization.

Table – 1

Country lists with six contributing factors to cybercrime

Country	Share of Malicious Computer Activity	Malicious Code rank	Spam Zombies rank	Phishing website hosts rank	Bot rank	Attack origin rank
USA	23%	1	3	1	2	1
China	9%	2	4	6	1	2
Germany	6%	12	2	2	4	4
Britain	5%	4	10	5	9	3
Brazil	4%	16	1	16	5	9
Spain	4%	10	8	13	3	6
Italy	3%	11	6	14	6	8
France	3%	8	14	9	10	5
Turkey	3%	15	5	24	8	12
Poland	3%	23	9	8	7	17
India	3%	3	11	22	20	19
Russia	2%	18	7	7	17	14
Canada	2%	5	40	3	14	10
South Korea	2%	21	19	4	15	7
Taiwan	2%	11	21	12	11	15
Japan	2%	7	29	11	22	11
Mexico	2%	6	18	31	21	16
Argentina	1%	44	12	20	12	18
Australia	1%	14	37	17	27	13
Israel	1%	40	16	15	16	22



Pie Chart 1: cybercrime in top 20 countries

V. CRIME ON THE INTERNET

Crimes committed on the Internet by using the Internet and by means of the same, are mainly called Internet crimes. According to David Wall, the term Cybercrime symbolizes to the occurrence of the harmful activities done with the digital devices mainly over the Internet. The Cybercrime practically doesn't refer to the law and it is the concept that is created by the media to a greater extend. In general term computer crime is a crime that encompasses crimes such as phishing, bank robbery, credit card frauds, child pornography, kidnapping of children by means of chat rooms, creation or the distribution of viruses and so on. All these are facilitated crimes related to computers. Some crimes which are committed on the Internet are exposed to the world and some are hidden until they perpetrated against someone or company. E-mail Related Crimes Electronic mail has rapidly become the world's most preferred means of communication. Across the globe, millions of e-mail messages are sent and received every day. E-mail, like any other means of communication, is also being misused by

criminals. It has become a powerful tool for criminals due to the ease, the speed of transfer and its relative anonymity. E-mail Spoofing: It is found in that an e-mail that appears to originate from one source while it is actually being sent from another source is called e-mail spoofing. Email spoofing is usually committed by falsifying the e-mail address of the sender and/or the name. to send an email, one usually has to enter the following information 1) The e-mail address of the receiver. 2) The e-mail addresses of the receivers (referred to as C for carbon copy). 3) The e-mail addresses of the persons who will receive a copy (referred as CC for carbon copy). 4) A subject for the message, which is a short title or a short description of the message. E-mail Defamation: Cyber defamation or cyber slander often proves to be very dangerous and even fatal for anyone with even a little knowledge of computers to become blackmailers often by threatening their victims through e-mails. E-mail Frauds: Financial crimes are commonly committed through e-mail spoofing. It is becoming easier to assume an identity as well as to hide one's own identity. The criminal knows very well that there is minimum chance of his being identified.

VI. WHO ARE CYBER CRIMINALS?

Kids(age group 9-16) Although it is hard to believe, kids can also be cyber criminals knowingly or unknowingly. The most amateur hackers comprises of teenagers. To these teenagers, it appears to be a matter of pride to be able to hack into a computer system or to a website. They may also commit the crimes without actually knowing that what they are doing is a crime. Organized Hacktivists Hackers who come together with a particular motive are called hacktivists. These groups mostly operate on a political basis. While in other cases, their motives may be social activism or religious activism or any other. Professional Hackers Extensive computerization has led to the storage of information in electronic form in business organizations. Hackers are employed by rival organizations to steal other industrial information and secrets which can prove to be beneficial for them. If hacking can retrieve the required information from rival companies, the fact that physical presence required to gain access is considered unnecessary. This also leads to the temptation of companies hiring professional hackers to do their dirty jobs.

VII. CONCLUSION

From this study made, it has been found that there are many ways and means through which an individual can commit crimes on cyber space. Cybercrimes are an offense and are punishable by law. In section 2, we have seen a brief discussion of the enlarging areas of cybercrimes. In section 3, we have seen the common types and areas where cybercrime occurs very frequently. We have also discussed the consequences of cybercrime that are causing tremendous financial losses in many countries, especially in the areas of sales and investments. Different fines and penalties have been laid down for this category of crime. Section 4 discusses about the different crimes on the net that are related to electronic mails. These crimes involve spoofing of mail, e-mail bombing and spreading malicious codes via emails. Furthermore, we have seen the different cyber criminals, ranging from the most amateur teenage hackers to the professional hackers that are often hired by rival organizations for hacking the into other company's system. It is therefore very important for every individual to be aware of these crimes and remain alert to avoid any loss. To ensure justice to the victims and punish the criminals, the judiciary has come up with some laws known as Cyber Laws. Hence, it is advisable to each and every individual to know these laws. Besides, the cybercrime cannot be simply called as a Technological problem. Instead, it is an Approach based problem because it is not the computers that are harming and attacking the organizations instead it is the humans who are exploiting the technology to cause the damage. Therefore, it is we who need to be alert to figure out the different approaches that such criminals can take. There is a need to have intellectual mindset to sense such situation that may lead to such damages. The solution to such crimes cannot be simply based on the technology. The technologies can just be one such weapon to track and put a break to such activities to some extent.

REFERENCES

[1]. P. Nirmala, T. Manimegalai, J. R. Arunkumar, S. Vimala, G. Vinoth Rajkumar, Raja Raju, "A Mechanism for Detecting the Intruder in the Network through a Stacking Dilated CNN Model", Wireless Communications and Mobile Computing, vol. 2022, Article ID 1955009, 13 pages, 2022. https://doi.org/10.1155/2022/1955009.

[2]. D. Sathyanarayanan, T. S. Reddy, A. Sathish, P. Geetha, J. R. Arunkumar and S. P. K. Deepak, "American Sign Language Recognition System for Numerical and Alphabets," 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), Chennai, India, 2023, pp. 1-6, doi: 10.1109/RMKMATE59243.2023.10369455.

[3]. J. R. Arunkumar, Tagele berihun Mengist, 2020" Developing Ethiopian Yirgacheffe Coffee Grading Model using a Deep Learning Classifier" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-4, February 2020. DOI: 10.35940/ijitee.D1823.029420.

[4]. Ashwini, S., Arunkumar, J.R., Prabu, R.T. et al. Diagnosis and multi-classification of lung diseases in CXR images using optimized deep convolutional neural network. Soft Comput (2023). https://doi.org/10.1007/s00500-023-09480-3

[5]. J.R.Arunkumar, Dr.E.Muthukumar," A Novel Method to Improve AODV Protocol for WSN" in Journal of Engineering Sciences" ISSN NO: 0377-9254Volume 3, Issue 1, Jul 2012.

[6]. R. K, A. Shameem, P. Biswas, B. T. Geetha, J. R. Arunkumar and P. K. Lakineni, "Supply Chain Management Using Blockchain: Opportunities, Challenges, and Future Directions," 2023 Second International Conference on Informatics (ICI), Noida, India, 2023, pp. 1-6, doi: 10.1109/ICI60088.2023.10421633.

[7]. Arunkumar, J. R. "Study Analysis of Cloud Security Chanllenges and Issues in Cloud Computing Technologies." Journal of Science, Computing and Engineering Research 6.8 (2023): 06-10.

[8]. J. R. Arunkumar, R. Raman, S. Sivakumar and R. Pavithra, "Wearable Devices for Patient Monitoring System using IoT," 2023 8th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2023, pp. 381-385, doi: 10.1109/ICCES57224.2023.10192741.

[9]. S. Sugumaran, C. Geetha, S. S, P. C. Bharath Kumar, T. D. Subha and J. R. Arunkumar, "Energy Efficient Routing Algorithm with Mobile Sink Assistance in Wireless Sensor Networks," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ACCAI58221.2023.10201142.

[10]. R. S. Vignesh, V. Chinnammal, Gururaj.D, A. K. Kumar, K. V. Karthikeyan and J. R. Arunkumar, "Secured Data Access and Control Abilities Management over Cloud Environment using Novel Cryptographic Principles," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ACCAI58221.2023.10199616.

[11]. Syamala, M., Anusuya, R., Sonkar, S.K. et al. Big data analytics for dynamic network slicing in 5G and beyond with dynamic user preferences. Opt Quant Electron 56, 61 (2024). https://doi.org/10.1007/s11082-023-05663-2

[12]. Krishna Veni, S. R., and R. Anusuya. "Design and Study Analysis Automated Recognition system of Fake Currency Notes." Journal of Science, Computing and Engineering Research 6.6 (2023): 16-20.

[13]. V. RamKumar, S. Shanthi, K. S. Kumar, S. Kanageswari, S. Mahalakshmi and R. Anusuya, "Internet of Things Assisted Remote Health and Safety Monitoring Scheme Using Intelligent Sensors," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ACCAI58221.2023.10199766.

[14]. R. S. Vignesh, R. Sankar, A. Balaji, K. S. Kumar, V. Sharmila Bhargavi and R. Anusuya, "IoT Assisted Drunk and Drive People Identification to Avoid Accidents and Ensure Road Safety Measures," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ACCAI58221.2023.10200809.

[15]. I. Chandra, G. Sowmiya, G. Charulatha, S. D, S. Gomathi and R. Anusuya, "An efficient Intelligent Systems for Low-Power Consumption Zigbee-Based Wearable Device for Voice Data Transmission," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10083856.

[16]. G. Karthikeyan, D. T. G, R. Anusuya, K. K. G, J. T and R. T. Prabu, "Real-Time Sidewalk Crack Identification and Classification based on Convolutional Neural Network using Thermal Images," 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2022, pp. 1266-1274, doi: 10.1109/ICACRS55517.2022.10029202.

[17]. R. Meena, T. Kavitha, A. K. S, D. M. Mathew, R. Anusuya and G. Karthik, "Extracting Behavioral Characteristics of College Students Using Data Mining on Big Data," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10084276.

[18]. S. Bharathi, A. Balaji, D. Irene. J, C. Kalaivanan and R. Anusuya, "An Efficient Liver Disease Prediction based on Deep Convolutional Neural Network using Biopsy Images," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 1141-1147, doi: 10.1109/ICOSEC54921.2022.9951870.

[19]. I. Chandra, G. Sowmiya, G. Charulatha, S. D, S. Gomathi and R. Anusuya, "An efficient Intelligent Systems for Low-Power Consumption Zigbee-Based Wearable Device for Voice Data Transmission," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10083856.

[20]. Revathi, S., et al. "Developing an Infant Monitoring System using IoT (INMOS)." International Scientific Journal of Contemporary Research in Engineering Science and Management 6.1 (2021): 111-115.