Phoenix: International Multidisciplinary Research Journal
Vol 3, No. 3, July-Sep, 2025
ISSN: 2583-6897

CYBERCRIME ANALYSIS AND INTERPRETATION: A REVIEW

Dikshendra Daulat Sarpate
Professor, Department of Artificial Intelligence & Data Science, ZEAL College of Engineering & Research, Pune, Email id -dikshendra@gmail.com
B. Sankaraiah
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: Shankar61186@gmail.com
B.Rani
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: rani@mrec.ac.in
Vemula Nikitha
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: nikitha479@gmail.com
Dr. Syed Umar
Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: syedumar@mrec.ac.in

Abstract— A survey was conducted to investigate the number of cybercrimes that were committed between the introduction of the blue box and the development of hacking-oriented operating systems. These operating systems provide novice hackers with the means to learn how to break into a variety of software technologies. At initially, cybercrime was utilized to introduce a large number of viruses and worms into the system in order to cause it to malfunction. Criminals operating online nowadays are interested in a variety of items, including but not limited to significant sums of money, extremely sensitive data and information, and top-secret files. In this paper, the evolution of cybercrime since 1970 is discussed, and an attempt is made to capture significant cybercrime events that have occurred along the way.

There are many different types of attacks that fall under the umbrella of cybercrime. Some examples of cybercrime include cyber extortion, cyber warfare, the spread of computer viruses or malware, Internet fraud, spamming, phishing, carding (fraud), child pornography, and the infringement of intellectual property rights. Due to the increasing number of cyberattacks that are occurring in the modern era, users of the internet are required to be aware of these dangers and to exercise caution when conducting business conducted online. The purpose of this study is to investigate the increases in cybercrime that have occurred in India as well as the measures that the Indian government has taken to tackle this issue.

INDEX - Cybercrime, Computer Crime, Cyberlaw, Cyber Crimes in India, worms, VIRUS, Hackers etc.

I. INTRODUCTION

At one time, the only way to understand a threat to the globe was to think of it in terms of the physical and real-world catastrophe that was produced by a single person or group of individuals. Thefts from banks, burglaries, gangsters, criminals from the underground, and other criminals were all significant dangers. Beginning in 1970, a new threat to civilization appeared in the form of 'hacking,' which was executed with the intention of breaking into a computer system [1]. Since that time, it has developed into one of the most essential and fundamental conditions for carrying out any other kind of attack. Cybercrime is the term that is most widely used to refer to it presently. There is a sizeable proportion of the criminal population that is comprised of cybercriminals. The term "cybercrime" refers to any illegal behavior that is carried out on a computer system, server, or database by utilizing a computer system and the internet to carry out a particular kind of activity. This includes activities such as downloading a file, spreading viruses, worms, phishing scams, botnets, or stealing millions of dollars. It is possible for

cybercriminals to attempt to steal money, useful information, top-secret datasets, and other items, depending on the cause for their attack. The fact that the perpetrators of cybercrime could be located in a territory that is completely different from where the crime is being perpetrated is the most dangerous component of this type of criminal activity [2]. Identity theft is a common form of cybercrime that involves users entering information that can be used to steal money from a person's bank accounts. This information includes a person's username, password, address, phone number, email address, bank account number, debit/credit card details, debit/credit card pin number, and other details that comprise a person's identity. Because to the rapid advancement of cybercrime, annual losses have increased from hundreds of millions of dollars to thousands of millions of dollars and even thousands of millions of dollars.

In this regard, every nation will have its own cyber legislation or Internet law in place to tackle the criminal activity that occurs online. Additional legislation, known as the Information Technology Act, 2000, was passed by the government of India. The entirety of the nation is included in the scope of this legislation, which establishes legal recognition for transactions involving electronic data interchange and other forms of electronic communication. The publication will provide a summary of the incidences of cybercrime that were reported and the individuals who were arrested on accusations of cybercrime during the years of 2010 and 2013. After that, the remaining parts of the paper are structured as follows: The industries that are susceptible to cyberattacks are discussed in Section II of this exposition. In Section III, an overview of the many types of criminal activity that were researched in the study is presented. The Information Technology Act of 2000 has a section that addresses the online offenses that have been reported as well as the individuals who have been arrested for committing these offenses. Section V investigates the arrests and reports of cybercrime that were made in accordance with the Indian Penal Code (IPC) between the years 2010 and 2013. In Section VI, we will examine cases that have been brought against offenders of all ages and provide a peep into the situation of cybercrime in each of the individual states and union territories under consideration [3].

II. CYBERCRIME'S EVOLUTION

The 1970-1979 Duration: The design of the blue box by Steve Wozniak and Steve Jobs (Apple founders), which was used to make free calls using a 2600 Hz whistle similar to that used by the operator's console, was one of the major technological crimes during this period. It controlled the switching in long dialling systems [3], interrupting ongoing calls and routing invaders' calls for free calling. Because of the limitations of the technology at the time, it was hard to track calls, which is why blue boxes were so popular among drug dealers.

The 1980-1989 Duration: The creation of the first computer virus by a Pakistani intelligent programmer, the Apple II boot virus, the establishment of CERT (computer emergency response team), the first bank computer theft worth 70 million dollars (national bank of Chicago), and the creation of the Morris worm by Robert T. Morris, Jr., a graduate student at MIT.

The 1990-2000 Duration: N The Electronic Frontier Foundation (EFF) was founded at the beginning of 1990, and it was there that the first ever online combat began- blocking phone lines, monitoring calls, and trespassing on each other's personal computers. A group known as the Dark Avengers unleashed the first polymorphic virus that affected data types and functions in 1992. Online piracy, identity theft assaults, spam, cyber stacking, cyberterrorism, Denial of Service (DoS) attacks, and botnet attacks were all new types of macro attacks in this decade. Melissa worm, the most expensive malware epidemic to date, was released near the conclusion of this decade. Towards the end, a few large extortions occurred, requiring a payment of roughly 100,000 INR or the hackers would expose all of the customers' credit card information[4].

During Year 2001: In comparison to past decades, this year experienced a significant surge in cybercrime. In the first month of the year, a new DoS (Denial of service) attack known as 'Servers' targeted

Microsoft, resulting in the shutdown of Microsoft's website for around 2 days, the Anna Kournikova virus was one of the most famous viruses, asking users to click on a link offering sexy pictures of Anna Kournikova, followed by the first polymorphic worm known as Code Red infecting thousands of machines, and the EU adopted a new cybercrime treaty [5].

The 2002-2004 Duration: This marked the start of the major cybercrime era. Things had not before resulted in large-scale financial losses. Roger Duronio, a sysadmin, developed a logic bomb that cost more than $3 million in repairs and damages. In terms of infected machines, the Klez.H worm has become the most widespread malware. SQL Slammer was the fastest-spreading worm in history in the start of 2003. The large reward of $250K offered by Microsoft for information regarding the creators of the MSBlastworm and the Sobig virus demonstrates the seriousness of these diseases. MyDoom worm, Netsky, Sasser, Bagel, and Sober worms were among the worms that hit Microsoft [6].

During Year 2005: With the news of the FBI's email system being hacked spreading in 2005, everything seemed unsecure and vulnerable, followed by the Paris Hilton T-mobie hack, Choice Point's 145K account information hack, Bank of America's 1.2M account information hack, and £220 million theft by hacking Sumitomo Mitsui Bank in London. One of the most common breakout viruses is Trojan horse malware, which spreads quickly and modifies the format of data files to something unintelligible, rendering them useless. [7].

The 2006-2008 Duration: This era witnessed a time constraint on attacks, which was known as Crime-Dot-9to5, which meant that the peak time of attacks was Monday through Friday between 9 a.m. and 5 p.m. NASA was obliged to restrict emails containing attachments because they were afraid of being hacked, which was one of the main events of 2006. In 2007, the email account of the US Secretary of Defense was stolen, and Estonia was subjected to a huge denial-of-service attack, which was followed by an attack on the Bank of India in September. In 2008, both the Republican and Democratic presidential campaigns' databases were hacked, followed by a Korean e-commerce site hack, which exposed Facebook's private photos via URL manipulations, and a DoS attack on Radio Free Europe[8].

The 2009-2012 Duration: Intruders attacked roughly 5 million computers in Israel's internet infrastructure to start the year 2009. A Twitter page was hacked at the end of 2009, displaying an Iranian message. After a Chinese search engine was hijacked in 2010, the identical Iranian message was shown. The Stuxnet worm was discovered in Iran and Indonesia, and it was designed to attack an Iranian nuclear site. A massive attack on Bank of America in 2011 resulted in the theft of 85k bank card numbers. TiGER-M@TE, a hacker, set a hacking record by hacking 70k domains with a single click. An open SQLi vulnerability was discovered in Facebook in 2012. Marriott and Foxconn were both hacked in a matter of days, resulting in a massive outage of these websites for a few days [9].

The 2013-2015 Duration: The year 2013 began with the hacking of Burger King's Twitter account and the publishing of the McDonald's logo. Following that, financial institutions in South Korea, as well as the broadcaster YTN, were infected, and they had to be shut down for several hours. Mt.Gox, a Bitcoin exchange, was hacked for $460 million in 2014, followed by news that the White House computer had been hacked. In the year 2015, a cloud service called hacking as a service reached its pinnacle. This year was the most profitable in terms of money theft, securities purchases, and so on. According to a survey done by Price Waterhouse Coopers, the average cost of the worst breach is £3.14 million [10].

Evolution of Cybercrime in India (2014–2024): According to projections, about 5.45 billion people, which is equivalent to 67.1% of the total population of the world, will have access to the internet by the year 2024. With over 2.9 billion users, Asia will account for the largest share of this userbase. This is mostly due to the fact that East and South Asian nations are dominant in this region. It is anticipated that Northern Europe will have the highest internet penetration rate, reaching roughly 97.5%. This is a reflection of the region's advanced digital infrastructure and ubiquitous accessibility. In contrast, regions

such as the Middle East and Africa have much lower rates of internet penetration than other regions [11,12]. It is possible to attribute this difference to a number of different issues, such as a lack of digital literacy, restricted technology resources, economic restraints, and an underdeveloped digital infrastructure. The widespread adoption of internet services in these locations is hampered by these problems, which contributes to the widening of the digital divide on a worldwide scale. For the purpose of encouraging fair access to information and participation in the global digital economy, it is still essential to address these concerns.

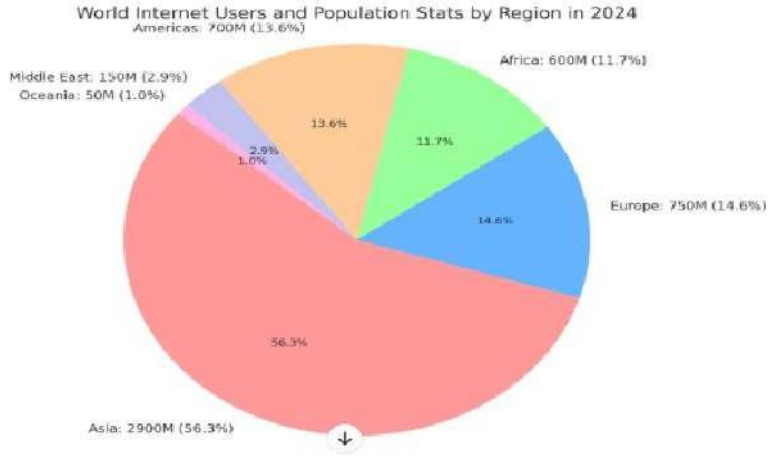

Figure 1: Internet users by world regions-2024 [13]

III. FIGURES OF CYBER CRIME EVOLUTION

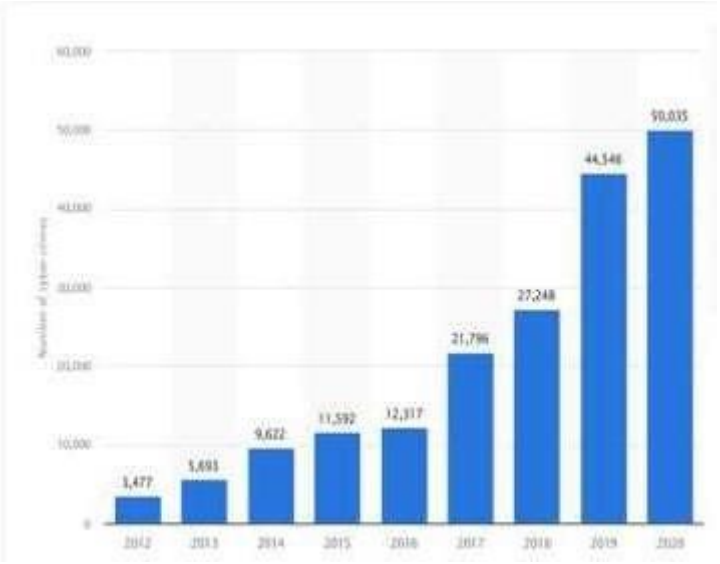

Fig 2: Number of Cyber Crime Cases

The figure 2 depicts the number of crime cases in India during year 2012 to 2020. The tremendous increment during 2017 to 2020 [14,15].

The figure 3 depicts how cyber threats have evolved over time. Ransomware, point-of-sale attacks, botnets, phishing attacks, cyber warfare, and network traversing worms are now the most commonly employed attacks. These kind of attacks are very common nowadays, and they affect millions of people all over the world [16,17].

Fig 3: Evolution of Cyber Crime

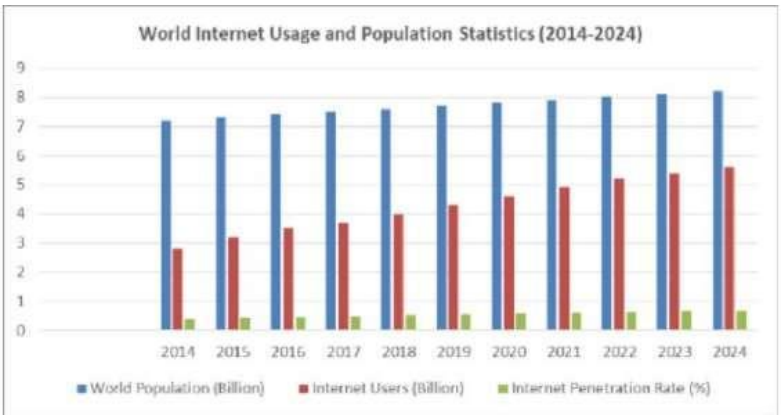

Fig 4: Cyber crime cases registered under the IT Act

The bar graph that is presented in Figure 4, which is labeled "World Internet Usage and Population Statistics (2014-2024)," provides a visual representation of the parallel rise of internet users and the expansion of the global population over the course of the ten-year period [18,19]. A constant increase in the world population is depicted by the blue bars, which show that the population is expected to reach 8.2 billion by the year 2024, according to estimates. On the other hand, the red bars illustrate the growth of the internet user base, which has increased dramatically from 2.8 billion in 2014 to 5.6 billion in 2024 because of the spread of the internet. According to the green line, the percentage of people who have access to the internet has significantly increased during the same period of time, going from 39% to 68%. A visual representation that emphasizes the growing significance of internet connectivity as a crucial component of global communication and access to information is presented here [20]. This not only represents the progress that has been made in digital infrastructure, but also the growing influence that the internet has had on the economic, social, and educational systems of multiple countries around the world.

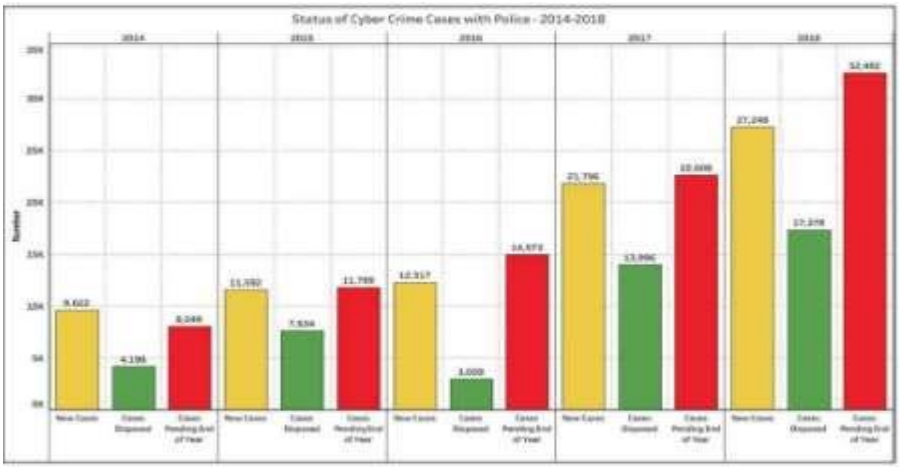

Fig 5: Top five cyber-crime heads under IT Act

Using the data in Fig. 5, the five largest crime heads are listed in decreasing order.

IV. CONCLUSION

As a conclusion, the rapid incorporation of technology into everyday life has resulted in a huge increase in the danger of cybercrime, which poses significant issues for individuals, organizations, and governments alike. Because the digital landscape is always shifting, it is imperative that cybersecurity measures be strengthened in a timely and comprehensive manner in order to safeguard sensitive data and digital assets. In this article, a full analysis of cybercrime is highlighted. Particular attention is paid to the development of innovative prevention strategies, the enhancement of internal security measures, and the categorization of essential cybercrime terms in order to provide a greater understanding of the impact that these terms have on digital systems and infrastructure. A survey that was carried out reveals that there has been a significant increase in the number of cybercrime occurrences that have occurred in India over the course of the last ten years. This highlights the urgent need for more robust legislative frameworks that are able to keep up with the ever-changing nature of cyber threats. It is essential to conduct a comprehensive public awareness campaign in order to educate citizens about the dangers and preventative measures that are related with cybercrime. According to the findings of a number of studies, public participation is an essential component in the process of establishing a culture of cybersecurity alertness. This culture is one in which citizens are not merely passive victims but rather active players in the process of protecting their digital life. Furthermore, financial fraud, phishing attacks, online harassment, identity theft, and ransomware occurrences are all revealing significant patterns, according to our review of recorded fraud cases across a variety of categories from 2014 to 2024. Each of these categories illustrates a changing environment of cybercrime, which has wider-ranging ramifications for society, ranging from monetary losses to emotional pain for victims. It is vital that all stakeholders, including government entities, business organizations, and individuals, remain informed and coordinated in their responses to these challenges as the digital ecosystem continues to evolve. This will ensure that a resilient framework for combating cybercrime in the future is established.

REFERENCES

[1] DataReportal. (2024). Internet use in 2024 – Global digital insights. DataReportal. https://datareportal.com.

[2] Naveen Sai Bommina, Uppu Lokesh, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Optimizing AI-Driven Security Protocols in IoT Networks Using Metaheuristic Algorithms", International Journal of Intelligent Systems and Applications in Engineering, IJISAE, 2024, 12(23s), 3339–3347.

[3] Statista. (2024). Global internet penetration and user statistics. Statista. Retrieved fromhttps://www.statista.com.

[4] Uppu Lokesh , Naveen Sai Bommina , Nandipati Sai Akash , Dr. Hussain Syed , Dr. Syed Umar. (2021). Deep Reinforcement Learning with Genetic Algorithm Tuning for Intrusion Detection in IoT Systems. International Journal of Communication Networks and Information Security (IJCNIS), 13(3), 582–595.

[5] Usman, M., Zubair, M., Hussein, H. S., Wajid, M., Farrag, M., Ali, S. J., ... & Habeeb, M. S. (2021). Empirical mode decomposition for analysis and filtering of speech signals. IEEE Canadian Journal of Electrical and Computer Engineering, 44(3), 343-349.

[6] Prometteur Solutions. (2023). Cyber Attacks in India: A Comprehensive and In-Depth Analysis. Retrieved fromhttps://www.prometteursolutions.com/blog/cyber-attacks-in

[7] McAfee. (2023). India's Cybercrime Landscape: Key Trends and Emerging Threats. Retrieved fromhttps://www.mcafee.com/blog/cybercrime-india-2023.

[8] Nandipati Sai Akash, Uppu Lokesh, Naveen Sai Bommina, Hussain Syed, Syed Umar, "Swarm Intelligence-Based Hyperparameter Optimization for AI-Powered IoT Threat Detection",

International Journal of Intelligent Systems and Applications in Engineering, (2024), 12(17s), 941.

[9] CyberPeace Foundation. (2022). India's Cybercrime Evolution: Challenges and Countermeasures. Retrieved fromhttps://www.cyberpeace.org/india-cybercrime.

[10] Press Information Bureau. (2023). Cyber-crime in India: Increasing trends and government initiatives. Retrievedfrom https://www.pib.gov.in.

[11] RS Supriya Khaitan, Divya Rohatgi, Sana Nalband, Tejali Mhatre, Shweta Patil, "Enhancing Essay Grading Efficiency and Consistency through Two-Layer LSTM Models and Attention Mechanisms", Journal of Information Systems Engineering and Management 10 (2), 191-202.

[12] Naveen Sai Bommina, Uppu Lokesh, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Optimized AI Models for Real-Time Cyberattack Detection in Smart Homes and Cities", International Journal of Applied Engineering & Technology, Vol. 4 No.1, June, 2022.

[13] Cyber Crime Reports. (2023). Analysis of cyber-crime trends in India: 2024 update. Retrieved fromhttps://www.cybercrimereports.in.

[14] Thakre N, Nimma D, Turukmane AV, Singh AK, Rohatgi D, Bangaru B (2024) Dynamic path planning for autonomous robots in forest fire scenarios using hybrid deep reinforcement learning and particle swarm optimization. Int J Adv Comput Sci Appl 15(9).

[15] Nandipati Sai Akash, Naveen Sai Bommina, Uppu Lokesh, Hussain Syed, Syed Umar, "Optimized Block Chain-Enabled Security Mechanism for IoT Using Ant Colony Optimization", International Journal on Recent and Innovation Trends in Computing and Communication, (2023), 11(10), 1226–1233.

[16] R. Gnanakumaran, Divya Rohatgi, A K Sampath, Nidhi Nagar, D. Amuthaguka, Raj Kumar Gupta, "Robust Extreme Learning Machine based Sentiment Analysis and Classification", 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), (2023), DOI: 10.1109/ICSSIT55814.2023.10061017.

[17] Habeeb, M. S., & Babu, T. R. (2024). MS-CFFS: Multistage Coarse and Fine Feature Selection for Advanced Anomaly Detection in IoT Security Networks. International Journal of Electrical and Electronics Research, 12(3), 780-790.

[18] K Sankar, Divya Rohatgi, S Balakrishna Reddy, "COX Regressive Winsorized Correlated Convolutional Deep Belief Boltzmann Network for Covid-19 Prediction with Big Data", Grenze International Journal of Engineering & Technology (GIJET), Grenze ID: 01.GIJET.9.1.547, © Grenze Scientific Society, 2023.

[19] Umar, Syed, Bommina Naveen Sai, Nagineni Sai Lasya,Doppalapudi Asutosh, and LohithaRani. "Machine Learning based Sentiment Analysis of Product Reviews Using DeepEmbedding." Journal of Optoelectronics Laser 41, no. 6(2022): 108-113.

[20] Singh, A., Gupta, M., Raj, A., Gupta, S. K., & Habeeb, M. S. (2020, December). TWDM-PON: The Enhanced PON for Triple Play Services. In 2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE) (pp. 1-5). IEEE.