ISSN: 2582-8118 *Volume 5, Issue 2; March 2025*

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYSIS IN SCIENCE AND ENGINEERING

Web: https://www.iarj.in/index.php/ijrase/index

3. Cyber Fraud Threatening Digital India User

Dr. Roy Anita Kumari Parmanand

Assistant Professor, Dept of Commerce,
Marwari College, Darbhanga, Bihar.

ABSTRACT:

The bulk of people now use the internet for their daily transactions. The number of internet users has increased dramatically, as have cybercrime rates. Cybercrime is defined as any crime committed utilizing a computer or a network. The threat of cybercrime is a constant and growing reality in both the private and professional sectors. With the advent of the internet, old crimes have taken on new forms. Cyber fraud is a big global concern, with India experiencing comparable problems. This issue has two main dimensions: technology exploitation and psychological manipulation. Cybercriminals expertly mix technological technology with psychological methods to fool people, frequently resulting in significant financial losses. Vulnerable people, particularly those with mental health issues, are commonly targeted by fraudsters who use their anxious emotions, worries, and sadness to trap them in fraudulent schemes. Cyber fraud victims come from a variety of socioeconomic levels, including both educated and unskilled folks. Fraudsters use cutting-edge technology and sophisticated psychological techniques to fool their victims, while many victims struggle to understand the quickly changing technological world and novel social engineering strategies. As cybercriminals become more sophisticated, stakeholders (financial institutions, law enforcement agencies, and consumers) must take a proactive and coordinated strategy to effectively address cyber fraud. The danger of cybercrime can be considerably lowered by improving cybersecurity measures, raising public awareness, and encouraging collaboration among relevant entities. Furthermore, understanding the psychological components that contribute to victimization can help build more effective preventative efforts.

KEYWORDS:

Cybercrime, Fraud, Digital User, UPI, E-Banking

1. Introduction:

The internet in India is expanding rapidly. It has created new opportunities in several fields such as entertainment, business, sports, and education. With the emergence and rising use of the internet, businesses have broken down barriers to local markets and are now reaching out to clients all over the world. Computers are widely utilized in businesses not just to process data, but also to obtain a strategic and competitive advantage. Computers may be used for both beneficial and detrimental purposes. India's digital transformation has been nothing short of extraordinary. From busy online marketplaces to a thriving digital startup environment, the internet has become an inseparable part of Indian life. This digital transformation has empowered citizens, accelerated economic growth, and established India as a worldwide superpower. However, this quick rise has left a long shadow: the ever-present menace of cybercrime. Millions of Indians have embraced the internet, engaging in e-commerce, receiving government services online, and communicating with loved ones all across the world. This digital inclusion has resulted in greater financial empowerment, improved communication, and expanded educational options. The rise of Indian tech behemoths and the thriving startup environment attest to the country's digital prowess.

Since 2016, when the National Payments Corporation of India (NPCI) created the Unified Payments Interface (UPI) system, digital transactions have undergone a revolutionary transformation. UPI fosters a cashless world by making it quick, convenient, and seamless to transfer money between bank accounts. However, as technology becomes more extensively used, there will undoubtedly be an increase in cybercriminals who use vulnerabilities to perpetrate crimes. This phenomenon underscores the need of understanding cyber security threats and having comprehensive cyber insurance policies.

It has been proven that in the first six months of 2017, at least one cybercrime was reported every ten minutes in India, up from every twelve minutes in 2016.India has experienced 1.71 lakh cybercrimes in the last 3.5 years, with 27,482 incidents so far this year, indicating that the overall number will likely exceed 50,000 by December. A study of data from 2013 to 2016 found that network scanning and probing accounted for 6.7% of all occurrences, whereas virus or malware accounted for 17.2%.

Categories of Cyber Crimes:

The principal types of cybercrimes can be broadly categorized into the following four classes based on their target and impacts:

1. **Crimes against Individuals:** These types of crimes are intended to hurt certain individuals. Hacking, cracking, email harassment, cyber-stalking, cyberbullying, defamation, dissemination of obscene material, email spoofing, SMS spoofing, carding, cheating and fraud, child pornography, assault by threat, denial of service attack, forgery, and phishing are some examples.
2. **Crimes against Property:** There are cybercrimes committed against an individual's property. They can be classified into intellectual property crimes, cyber-squatting, cyber vandalism, hacking computer systems, computer vandalism, computer forgery, transmitting viruses and malicious software to damage information, Trojan horses, cyber trespass, Internet time thefts, robbery or stealing money during money transfers, and so on.
3. **Crimes against Government /Firm /Company /Group of individuals:** These crimes include cyber terrorism, unlawful information possession, pirated software distribution, web jacking, salami attacks, logic bombs, and so on. The offenders in these cases want to terrify the residents of the country.

Objectives:

- To study cyber fraud threatening
- To study rising cybersecurity incidents
- To study investment in cybersecurity
- To analyze cyberattack and its loss
- To study key factors measuring the level of cyber risks
- To study methods used in mobile app phishing attacks

Review of Literature:

Aparna & Chauhan (2012) In their study, the authors performed research on cybercrime awareness in Tricity and discovered that increasing awareness may be achieved by emphasizing cybercrime, which can be an effective method for reducing or preventing cybercrimes. They also determined that it is the obligation of both internet users and the government to maintain a safe, secure, and trustworthy computing environment.

Mehta & Singh (2013) The author performed a survey to assess awareness of cyber regulations in Indian society. He discovered a considerable disparity in the level of awareness among male and female internet users. Male netizens are more aware of cyber regulations than female users.

Agarwal (2015). In her paper, the author explored the many types of cybercrime and the cyber laws enacted to combat them. Her goal was to determine whether internet users are aware of cybercrimes. She also stated that it is the responsibility of all internet users to be informed of cybercrimes and cyber regulations.

According to Kaur, M., et al. (2017), effective cybercrime combat requires multidimensional collaborations between the public and private sectors, including law enforcement agencies, the information technology industry, information security organizations, internet companies, and financial institutions. Cybercriminals, unlike their corporeal counterparts, do not compete for power or control. Instead, they collaborate to improve their talents and help each other uncover new opportunities.

In its publication "Raju and the Forty Thieves" (2021), the Reserve Bank of India provided forty stories highlighting various fraud cases reported to the bank, including those from the RBI Ombudsmen and the Consumer Education and Protection Department (CEPD). Each story offers easy advice on how to avoid similar incidents. The character "Raju" is an ordinary, trusting citizen who takes on numerous roles—such as a senior citizen, a farmer, or a carefree individual—to allow readers from varied backgrounds relate to him in different life situations.

In his study, Shah, R. (2019), explores the different motivations for cybercrime, such as financial gain, desire for fame, fun, sexual exploitation, blackmail, company development, trafficking in illicit content, revenge, and pranks. A crucial benefit for these criminals is their ability to operate online in relative anonymity, making them difficult to track down.

The worldwide nature of the internet hinders efforts by cyber officers and law enforcement, as crimes can occur anywhere in the globe, and tracing such actions requires many locations, making it increasingly difficult to catch cybercriminals. According to a study (Soomro and Hussain, 2019), PC users spend more than 12 minutes on social networking sites during an hour-long online session. In comparison, mobile internet users spend more than 18 minutes on social networking sites.

However, logging into social media and scrolling through the content on a regular basis is not recommended because it is likely to lead to a syndrome known as "Fear of Missing Out (FOMO)," for which many people have sought professional help. According to one study, the suppression of cybercrime can have a significant impact on individuals, resulting in emotional anguish and a diminished motivation to participate in cyberspace. Cybercrime has a significant impact on youth, causing depression to the point of self-harm. Girls afflicted by cybercrime have experienced extreme mental torment (Malar, 2012).

With so many websites providing a diverse spectrum of content, consumers must pay special attention to the source. This is especially critical given previous examples of disinformation, data breaches, and the spread of fake news. Furthermore, to safeguard themselves, visitors should double-check the website's orthography, URL, and HTTP address. Furthermore, public Wi-Fi should be avoided in places like restaurants, train stations, airports, and hotels because it is vulnerable to man-in-the-middle attacks, which allow hackers to easily intercept and access personal information shared between a user and an application. To reduce this risk, it is best to avoid using public Wi-Fi completely. (Deora & Chudasama, 2021).

Research Methodology:

The researchers employed an exploratory research technique based on previous literature from relevant journals, yearly reports, newspapers, and magazines, which covered a wide range of academic literature. Research methodology is a systematic approach to solving a research challenge.

It might be defined as the study of how scientific research is conducted. In it, we look at the many phases that a researcher typically takes when researching an issue, as well as the reasoning behind them. The researcher must be familiar with both the research methodologies and procedures, as well as the approach.

Result and Discussion:

According to the Ministry of Electronics and IT, Government of India, financial fraud incidents affecting ATMs, cards, point-of-sale (POS) systems, and Unified Payment Interface (UPI) were reported in 2016, 2017, and 2018 [7]. In 2015-16, 2016-17, 2017-18, and 2018-19, the Reserve Bank of India (RBI) reported 1,191, 1,372, 2,059, and 921 cases of fraud involving ATM/debit cards, credit cards, and internet banking. In 2019, 394,499 cyberattacks were reported, but they are expected to increase by at least 300 percent by 2020, reaching 1,158,208. Figure 1 depicts the increased number of cybercrimes in past years.

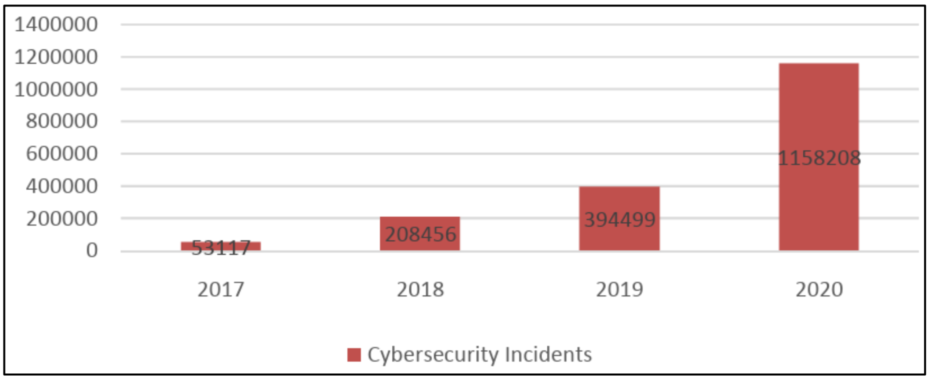

Figure 1 Rising cybersecurity incidents from 2017 to 2020
Source: (https://efaidnbmnnnibpcajpcglclefindmkaj/https://ijarsct.co.in/Paper1372.pdf)

The severity of cybersecurity challenges in the present electronic era is obvious from the figures, which show that only 21.8 billion USD was invested in cybersecurity in 2021, compared to 5.1 billion USD in 2017, 5.9 billion USD in 2018, 8.3 billion USD in 2019, and 8.9 billion USD in 2020. Furthermore, according to the data, the fourth quarter of 2021 had the highest amount of 7.8 billion USD in cybersecurity investment, as shown in Figure. Figure 5 indicates that cybersecurity spending is expanding year after year, with substantial growth expected by 2021.

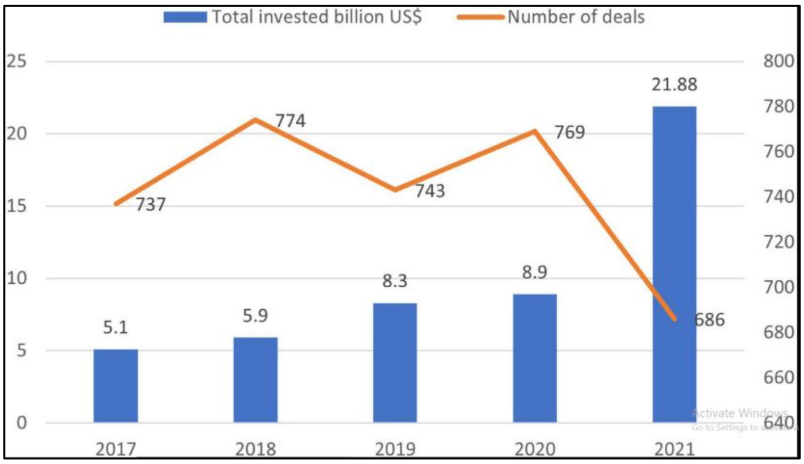

Figure 2 Investment in cybersecurity
Source: (Liu Xiang , Ahmad Sayed Fayaz , Anser Muhammad Khalid , Ke Jingying , Irshad Muhammad , Ul-Haq Jabbar , Abbas Shujaat,Cyber security threats: A never-ending challenge for e-commerce,Volume 13 - 2022, https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.927398 DOI=10.3389/fpsyg.2022.927398)

Cyberattacks have more than doubled since the outbreak. While most organizations have incurred relatively minor direct losses as a result of cyber assaults, some have suffered far more. The probability of suffering a cyber-attack and incurring severe losses has grown.

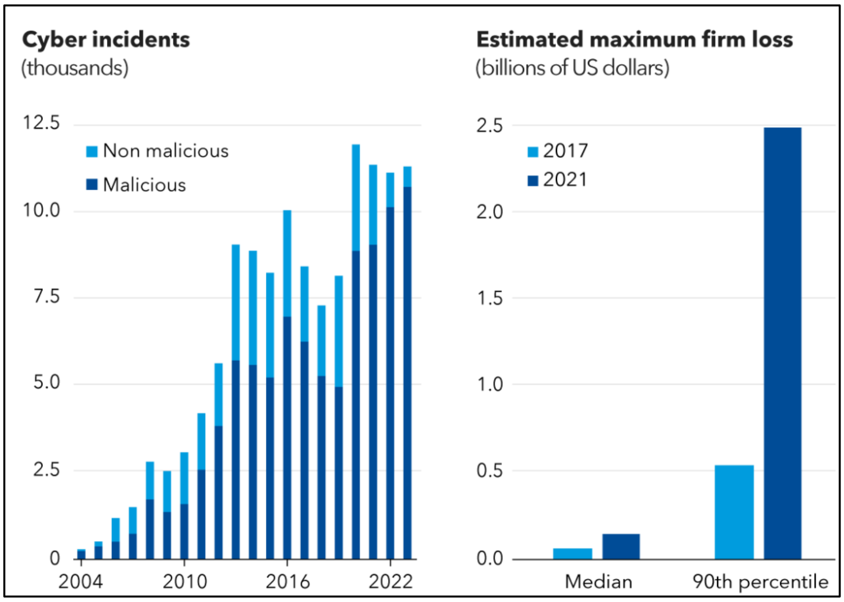

Figure 3 Cyberattack and Loss

Source: (Advisen Cyber Loss Data;Capital IQ; and IMF staff calculations)

Modern risk management strategies rely on the probability of threats, damage, and vulnerabilities. However, in most cases, information security experts conduct assessments using verbal formulations and then link them with numerical values based on their own experience. Today's risk analysis approaches focus solely on technological weaknesses, which prevents a thorough assessment of the economic consequences.

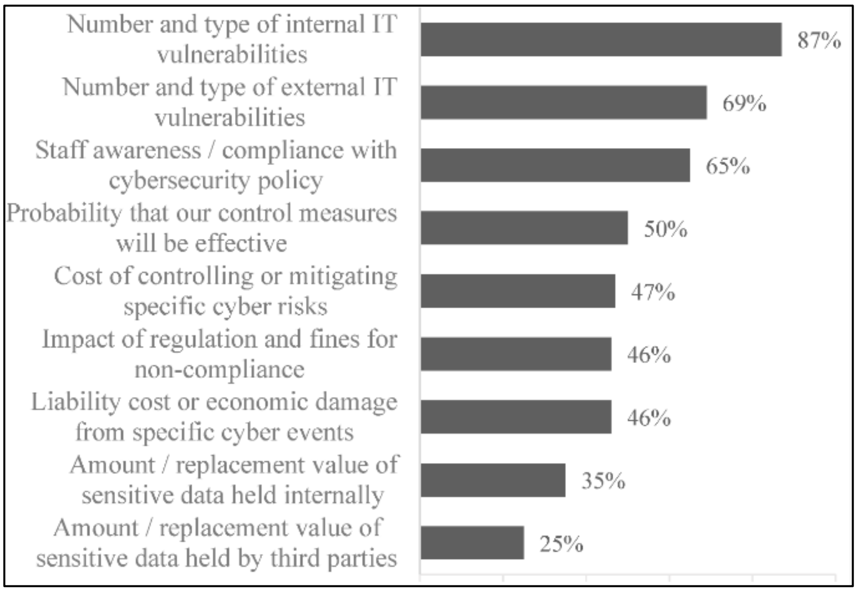

Figure 4 Key factors measuring the level of cyber risks

Source: *(The Marsh Microsoft 2019 Global Cyber Risk Perception Survey)*

Figure 5 depicts the measurement of cybercrime by kind. Viruses are the most common, whereas financial fraud accounts for the fewest. There are eight varieties of cybercrime, ranging from tiny to huge.

Between 1998 and 2000, estimated reported damages from cybercrime increased by $129 million. It's easy to understand why sales of security software and devices have increased, as indicated in the following figure.

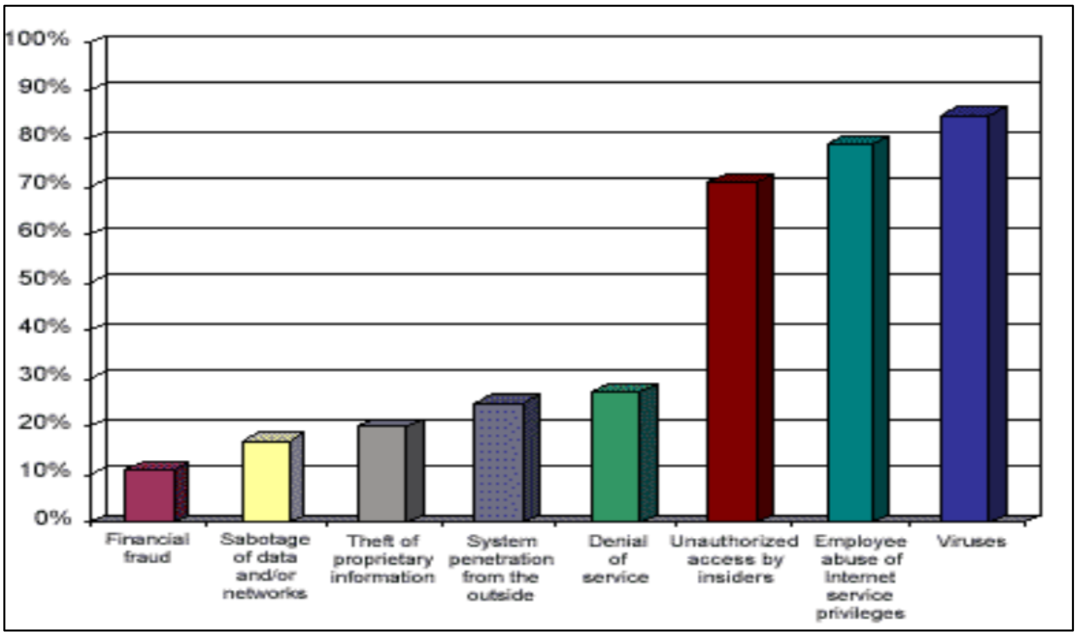

Figure 5 Types of Cybercrimes

Source: *(Ramadani, Suci & Siahaan, Andysah Putera Utama. (2018). Impact of Cybercrime on Technological and Financial Developments. 4. 341-344.)*

The convenience of mobile apps has transformed our lives. However, this convenience comes with a hidden risk: mobile app phishing attempts.

In the past, India has seen an increase in similar attacks, underlining the need for vigilance in the mobile app ecosystem.

Mobile app phishing assaults can have terrible implications. Malware that has been downloaded has the potential to steal important information such as bank account numbers, passwords, and contact information.

This can result in financial losses, identity theft, and account hijacking. Victims may sometimes feel frustrated and helpless when recovering from a cyberattack. The strategy utilized in Mobile App Phishing Attacks is shown in Figure 6.

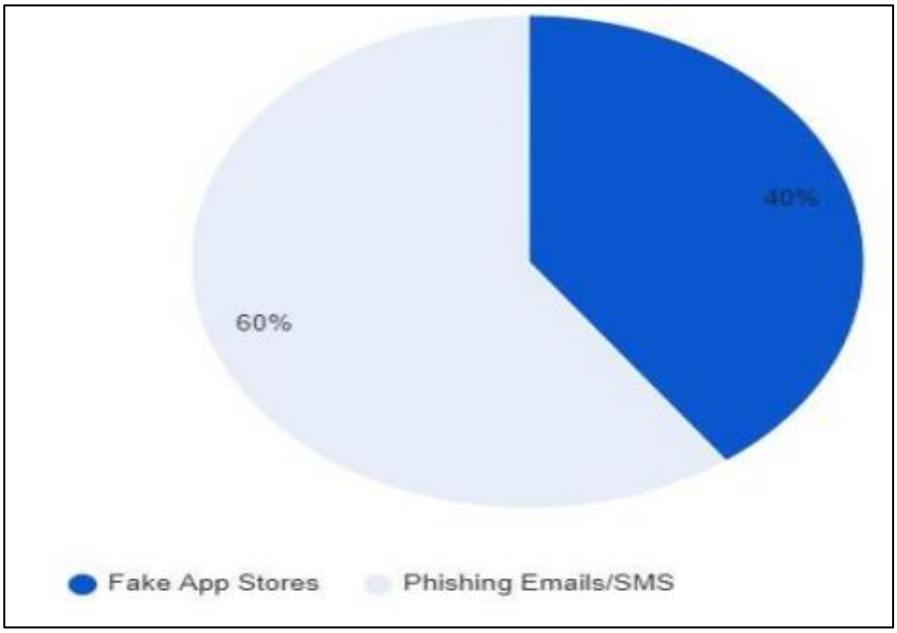

Figure 6 Methods Used in Mobile App Phishing Attacks

Source: (Dr. Naresh Mahipal , Dr. Jyoti Garg. (2021). An Analytical Study On Cyber Crime In Indian Marketing. Elementary Education Online, 20(6), 6560–6570. Retrieved from https://ilkogretim-online.org/index.php/pub/article/view/8048)

Conclusion:

As the number of internet user’s increases, so does the number of cybercrimes. There are different types of cybercrimes that occur in daily life. However, people are unaware of all such sorts. The majority of people just know about hacking and viruses/worms. They are unaware of phishing, defamation, identity theft, cyber stalking, and other cybercrime. Today's world requires understanding of these internet-related crimes. The possibility for money laundering fraud in India's UPI system highlights the importance of improving regulatory oversight and cybersecurity safeguards. India has the potential to protect its financial system and mitigate the dangers associated with cybercrime by deploying new technical solutions, engaging with stakeholders, and closing legislative gaps. To fully solve these concerns, users, technology providers, financial institutions, political entities, and society must all collaborate on a constant basis. Internet users were bombarded with spam emails, scam calls, and emails requesting personal information such as their cell phone number, bank account, and address. It is everyone's responsibility to be aware of fundamental cyber security. Cyber security refers to the technologies and techniques used to safeguard computers, networks, and data from unwanted access and attacks provided via the internet by cyber criminals. The government is also making measures to curb cybercrime. It enacted cyber laws to educate people about various cybercrimes and cyber security. The Information Technology (IT) Act of 2000 addresses cyber-related crimes. Not only should the government, but also the people, work together to apprehend criminals. People who have been victims of any of these cybercrimes should come forward and register a complaint with the appropriate cybercrime cells.

This will undoubtedly assist to combat cybercrime. As a result, cybercrime and security awareness is more important than ever. This study emphasizes the critical necessity for a multifaceted approach to cybersecurity, highlighting the relevance of not just technological solutions but also the human factor in combating cyber fraud.

References:

1. Aparna and Chauhan, Meenal (2012), Preventing Cyber Crime: A Study Regarding Awareness of Cyber Crime in Tricity. International Journal of Enterprise Computing and Business Systems, January, Vol 2, Issue 1
2. Mehta, Saroj and Singh, Vikram (2013), A Study of Awareness aboutCyber laws in the Indian Society. International Journal of Computing and Business Research, January, Vol.4, Issue. 1.
3. Aggarwal, Gifty (2015), General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering. Vol 5, Issue 8.
4. Reserve Bank of India (2021). Raju and the Forty Thieves – A Booklet on Modus Operandi of Financial Fraudsters, URL: https: //www.rbi. org.in/commonperson/English/Scripts/BasicBankingNew.aspx, Accessed on 25 - 10 - 2024.
5. Shah, R. (2019). Cyber Crimes in India: Trends and Prevention. International Journal of Research and Analytical Reviews (IJRAR), 6 (1), 2348 - 1269.
6. Kaur, M., Kaur, G., Raina, C. K. (2017). Cyber Crime and Its Preventive Measures. International Journal of Advanced Research in Computer and Communication Engineering, Vol.6, Issue 3, DOI:10.17148/IJARCCE.2017.63214
7. Halder D, Jaishankar K. Use and Misuse of Internet by Semi-Urban and Rural Youth in India: A Baseline Survey Report (2013). Available at SSRN 2378968. 2014.
8. Humayun M, Niazi M, Jhanjhi NZ, Alshayeb M, Mahmood S. Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering. 2020 Apr;45(4):3171-89.
9. Sohail SS, Siddiqui J, Shakil MT, Ubaid S, Ahmed J, Alam MA. Sustainable Approach for University Ranking System. ICIDSSD 2020. 2021 Mar 3:257
10. Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. Appl. Comput. Syst., 24(1), 9-17
11. Malar, M. N. (2012). Impact of cybercrimes on social networking pattern of girls. international Journal of Internet of Things, 1(1), 9-15
12. Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. Journal of Communication Engineering & Systems, 11(1), 1-6
13. D. J. Neufeld, “Understanding Cybercrime,” in 2010 43rd Hawaii International Conference on System Sciences, 2010, pp. 1–10.
14. S. Haryati, A. Ikhwan, D. Arisandi, Fadlina, and A. P. U. Siahaan, “Quality Assurance in Knowledge Data Warehouse,” Int. J. Sci. Res. Sci. Technol., vol. 3, no. 6, p. 239–242], 2017.
15. A. Lubis and A. P. U. Siahaan, “Network Forensic Application in General Cases,” IOSR J. Comput. Eng., vol.18, no. 6, pp. 41–44, 2016.