Threats, Effects, and Awareness of Cybercrime: A Survey

Moulik Singh Arora[1], Preksha J Dadhania[2]

[1]School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore 632014, Tamil Nadu, India
[2]School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore 632014, Tamil Nadu, India

---***---

Abstract - The emergence of the digital age has ushered in unprecedented connectivity and convenience, but it has also brought about a surge in cybercrimes, posing significant challenges to security. Criminals exploit vulnerabilities in cyberspace to access sensitive information, perpetrate fraudulent activities, and undermine trust in online interactions. Despite the pervasive impact of cyber threats on various facets of society, awareness levels among the general populace remain a critical concern. This paper presents findings from a comprehensive survey aimed at assessing public awareness of cybercrimes and cybersecurity measures. The survey, conducted through a structured questionnaire, solicited responses from a diverse demographic sample, encompassing individuals' background information and their perceptions of cyber threats. Participants were queried on their familiarity with prevalent cyber scams, including phishing, email spoofing, lottery scams, credit card frauds, investment scams, vishing frauds, and gaming frauds. Key findings reveal gaps in awareness and understanding of cyber risks, underscoring the need for enhanced education and vigilance. Furthermore, insights into participants' responses regarding their experiences with cybercrimes, including measures taken to address incidents and financial losses incurred, shed light on the real-world impact of cyber threats. In conclusion, this paper emphasizes the importance of proactive measures to safeguard against cybercrimes and offers recommendations for bolstering cybersecurity awareness and resilience in the digital age.

Key Words**:** Cybercrime, Scams, threats, Analysis, Awareness.

1. INTRODUCTION

India, as we are all aware, is the second-most populated nation in the world, with more than 139 crores, and has hundreds of millions of internet users. There would be roughly 825.30 million active users in India in March 2021, according to the telecom regulatory authority of India with a monthly data use average of more than 20 GB. All of this is made possible by the affordability and accessibility of the internet in India. Cybercrime, commonly referred to as computer crime, is the use of a computer for illicit purposes, such as fraud, the trafficking of child pornography and other intellectual property, identity theft, and privacy violations. International cyber laws have been created as a result of the global character of cybercrimes. Any fraudulent activity carried out through a computer or computer data is referred to as cyber fraud. Fraudsters can access their victim's personal information, online accounts, and bank accounts by using the internet. They can then sponsor terrorism with the cash and knowledge gained from this. Since cybercrime is related to digital devices, no amount of precaution and safety and completely prevent breaches, data leaks, etc. India reported 52,974 cases of cybercrime in 2021.

The fact that the first cybercrime ever documented occurred in 1820 is astonishing. Cyber or digital crime is thought to have originated in India around 2005. The most common misconception about cyber scams is that people think it only

affects victims financially, which is not always true. Along with financial loss, some victims also experience negative impacts on their mental health, physical health, and even on their personal relationships. Some victims suffer emotional distress even when there is no financial loss faced by them. Due to these over-rising scams, people find it difficult to trust each other even with the smallest things. Cybercrime is a topic of concern not only in India but in other foreign countries as well. India recently experienced a malware attack from Chinese hackers in the "All India Institute of Medical Science" (AIIMS), Delhi on 23rd November 2022. The report generation, appointment system, billing counters, smart labs as well as digital hospital services including outpatient and inpatient were affected due to the attack on the servers. The attackers were successfully able to get through 5 physical servers out of 100 (40 real and 60 virtual). The Central Forensic Lab (CFL) was given the responsibility for finding the source of the hack. Cyber-attacks are not just centered to big companies but to everyone who holds some kind of sensitive information that can be beneficial for the attackers. In January 2022, the International Committee of the Red Cross (ICRC) faced a cyber-attack that compromised the information of more than 515,000 vulnerable people from at least 60 Red Cross and Red Crescent Societies. Many such cybercrimes keep happening every day. There are various types of cybercrimes. Cybercrimes are not restricted to one form.

[1]Some of the most common cybercrimes are:

- *Phishing*

Phishing is an act of acquiring confidential information such as a username, credit card details, or password by pretending to be an authorized source. In which an attack is done through the link which is usually sent to victims through the mail.

- *Email spoofing*

It is a type of cyberattack where the hacker sends mails with forged senders' address. The mail usually contains a link, attachment, or some other malicious content. When the user clicks on the link, he is redirected to a phishing page, and this way a hacker can get the user's personal details.

- *Lottery scams*

It is a type of scam where the user receives an unexpected mail, call, or message stating they have won a prize/lottery. The users are asked to call an agent and when this happens, they are asked to pay money as fees in order to collect their lottery. The user gives his personal bank details and this way the hacker can now make transactions.

- *Credit card fraud*

In credit card frauds, unauthorized users gain access to people's card details. This could be done by various means like stealing, skimming, etc

- *Investment scam/Money Double*

This happens when scammers try to trick people into investing money in cheap schemes like money double where they ask us to provide a big sum of money in exchange for doubling it in a few days, or insisting people to buy a certain property at cheap price.

- *Vishing fraud*

These scams are executed over phone calls. An unauthorized person tricks people into revealing personal information like bank details.

- *Gaming fraud*

This happens when people have to pay a sum of money in order to get prizes in a game. People's bank details are captured by a 3rd person with the help of phishing pages.

2. RELATED WORK

It is necessary to analyze the number of people that fall victim to cyber-attacks as it is an issue of concern at a global level. The research papers till now have explained either the different types of cybercrimes, conducted a survey to understand the effect of cybercrime on people, or discussed preventive measures to safeguard themselves from cyber-attacks, but no paper has included all 3. Keeping this in mind this paper explains the different types of cybercrimes, shows the analysis of the survey that was conducted on cybercrime among 146 people who belonged to different regions and whose ages varied from 18 years to 60+ years, and also mentions the suggestions that can be followed to prevent being a victim to these scams. The convenience sampling method was used to collect the survey from the study population [2]. The experiences shared by responders and the conclusions based on them are mentioned in this research paper along with their corresponding percentages and appropriate graphs. Some papers that were reviewed for the study are mentioned below :

In [3], researchers have examined attacks targeting the sensing components from the perspective of cyber-physical interaction. A generalized system model of CPS and an attack model for every attack is developed, providing a new way to understand and motivate effective defenses based on the systemized threat model. The two key elements that make it possible to interface the cyber and physical worlds are sensors and actuators. Traditional network or software attacks are not like cyber-physical attacks. IoT security flaws can result in widespread classical security issues like distributed denial of service (DDoS) attacks. Spoofing or denial of service can result from signal injection attacks. Some sensors, including microphones, accelerometers, and gyroscopes, have been vulnerable to information leakage and signal injection attacks.

Phishing email attacks are among the most common types of cybercrime and top security risks as explained in [4]. Most social engineering breaches occurred in the public administration sector, followed by other professional services. Older workers are the least vulnerable to phishing scams, and men are twice as likely as women to fall for them. The personality characteristics of the individual are directly connected with their chance of getting phished. Conscious users were found to negatively affect heuristic processing, making them less vulnerable to phishing on social networking sites.

Researchers defined the goal of [5] as establishing a link between user behavior on online social networks (OSNs) and security and privacy. OSN users frequently engage in certain actions that make them easy targets for hackers. These actions could include calling, chatting, and sending data across OSNs as well as clicking on links and alluring videos and photographs. According to survey findings, social media usage among Iraqis is higher than that of Turks. For all sorts of attacks that were considered in this study, social media users in Iraq are more vulnerable than users in Turkey.

In order to assist investors in making decisions about their investments in a variety of different situations, a methodology for quantitative risk analysis is proposed in [6]. Data collection is difficult because external researchers and organizations sometimes lack a fundamental grasp of their systems. A thorough, rational strategy can help firms regularly improve their cybersecurity. Cyber risk management's quantitative help has a lot of potentials. Cyber threats change as new attackers emerge but get more familiar with experience and time. The model presented in this paper is wide enough to accept these unique circumstances once information on additional inputs is acquired.

In [7], the authors explained a cyber-physical system (CPS) which is a typical product of Industry 4.0. CPS enables virtual world analysis of data gathered from the real world. CPSs have numerous uses, including smart grids, healthcare, aviation, digital manufacturing, and robotics. The idea of attacking CPSs online is becoming more popular. Power generation facilities, transmission and distribution facilities, consumer facilities, control facilities, and communication networks make up a typical CPS. An assault known as a ransomware attack disables or restricts users' access to their files and systems. Such assaults result in severe financial losses in addition to harming a system's availability and confidentiality. The distance between theoretical findings and actual applications is still very large. Many scholars attempt to incorporate computer science and model-based methodologies to fill it.

In, 1998, protesters launched a denial-of-service attack on the Mexican president's website using a programme called FloodNet. The accessible datasets that were used by earlier investigations have been thoroughly reviewed in this paper. A combination of traditional and fuzzy sets is called fuzzy logic. It gauges the degree of veracity, or how strongly it can be inferred that a given object is a part of a set. Due to the uncertainty and doubt surrounding the gathering of evidence, this logic is required for detecting cybercrimes as discussed in [8].

Cyberbullying is the deliberate act of cyber-bullying carried out through electronic means such as e-mail, social media, images and digital messages [9]. Autistic adolescents are particularly vulnerable to cyberbullying due to specific characteristics of their disabilities. 78 autistic adults completed at least 70% of the questionnaires. Twenty-nine participants were male (37.2%), 43 were female (55.1%) and 6 preferred not to state their gender. Participant ages ranged from 18 to 59 years (M = 29.3, SD=9.7). Just under one-half (48.7%) were currently in education. Cyberbullying victimization and cyber-aggression were measured using the ECIPQ, which measures self-esteem.

Johnson and Nikolovska [10] used monthly counts of hacking, and online– and doorstep–fraud offenses committed within the UK for the period 1 January 2014 to 31 August 2021. COVID-19 restrictions limited the rate at which, offenders could approach targets on the doorstep. Tier 4 restrictions were essentially lockdown rules as people were asked to stay at home and non-essential shops and businesses were closed. Data shows that crime and internet sales were higher during the pandemic, but doorstep crime and mobility were lower. For hacking, there is an initial peak in crime which mirrors the trends in online sales, but levels of hacking do not subsequently exhibit the same peaks observed for online shopping fraud. Cybercrime accounts for a substantial amount of all crime and this share appear to have increased during the pandemic. The paper concludes with a discussion of the findings and their implications for cybercrime prevention in the 21st century.

As explained by Kaur and Munish [11], in July 2021, there were 4,80 billion social media users globally, representing a 5.7% annual growth as 7 million new users sign up every day (Digital Around the World, 2021). One of the serious issues that need to be solved is cyberbullying. Cyber bystander intervention and peer-to-peer interaction can help to reduce the number of victims of cyberbullying. 60% of the respondents are students, and 80% of them are in the age range of 17 to 24. The most frequently used app among students is WhatsApp. 50% of respondents consider posting harmful content on social media, threatening someone, and photographing or distributing embarrassing pictures to be serious cyberbullying behaviors. 58.2% of students don't know where to report bullying, and more than half are unaware of cyberbullying rules.

The authors of [12] claim that increasing security awareness is the best method to lower danger in cyberspace. In 2019, 73.4% of Serbians utilized the Internet, making up more than half of all Internet users worldwide. Researchers from the Faculty of Security Studies and the University of Belgrade carried out the study. The majority of the inquiries were drawn from a Pew Research Center poll that was conducted in 2016. Although 99.3% of students use social networking sites like Facebook and Twitter, the majority of them (73.5%) have never experienced a security breach. Due to the difficulty of remembering complex passwords, 54.4% of participants opted to use less secure passwords. Public Wi-Fi networks are extremely weak points that hackers can readily exploit.

The five-function model presented by the National Institute of Standards and Technology (NIST) paradigm for cyber security: Identify, Protect, Detect, Respond, and Recover is explained in [13]. The flow observation method gathers the packets that share the five-tuple of source and destination IP addresses rather than inspecting every single packet. Compared to the conventional data analysis method, this method is quicker, less invasive to privacy, and requires less storage. SIEMs are devices that can gather, aggregate, and store events produced by a system. Real-time data collecting from the host level is made possible via endpoint detection and response (EDR). Elasticsearch, Logstash, and Kibana are the three open-source applications that make up the ELK-Stack. It has been demonstrated that ELK-Stack works well for both organizing and collecting logs as well as for cyber incident detection. Logs are a sign of the harmful activities used to guess a system password in order to take over control of it.

According to Syafitri et al. [14], pop-up models can present users with information that they must promptly click on in order to access, such as a virus that infects their computers. Education and training of potential victims is the best method for preventing them. One of the defenses against social engineering attempts is to launch a health campaign. Analysis of the penetration testing described in this study is advised, especially when conducting a cyber operation. Text mining, time profiles, statistics, composite behavioral, cross-platform, and behavioral profiles are all possible methods for detecting social engineering. The use of a scenario-based experiment or the absence of an actual attack study was the research's shortcomings.

The Balloon Risk Assessment Trial (BART) analyses a person's potential for reward and loss in order to gauge their risk-taking behavior [15]. A total of 62.2% females (84 participants) and 37.8% males (51 participants) were involved in the test. There were 43 questions in total, and the examinations were supposed to take 20 minutes to complete. The purpose of the paper was to determine how behavior during the various phases of a phishing attempt affected the outcome. 22 were risky users and 10 were high-risk users out of the 97 persons involved. In the second stage of phishing, women are marginally more susceptible than males. A phishing webpage was also created which asked users for 1 billion dollars.

Tsakalidis and Vergidis [16], provide a hybrid schema-based incident description that can be adjusted to appropriately include and include different cybercrime incidents. By having such a mechanism, it is possible to:
1) better comprehend a particular incident;
2) accurately classify and monitor the associated criminal offense; and
3) take appropriate action in terms of developing countermeasures and policies. Cybercrime may be better understood, tracked, and grouped when it is approached methodically. This study suggests a two-level framework for categorizing cybercrime offenses based on the original typology developed by the European Union. According to the researchers' suggestion, the authors are working on automating the suggested approach utilizing the XML-based Structured Threat Information Expression (STIE).

Another study [17] explains that a portion of the internet called the Dark Web is not included in search engine indexes. Data breaches, illicit drug use, pornography, human trafficking, and other unlawful activities make up 57% of the dark web's operations. About $1.5 trillion was made in total in 2018 as a result of cybercrime. This research serves as the foundation for creating a prototype to identify cyber threats and produce a suitable reaction. The majority of traffic from different browsers to hidden Dark Web sites is for viewing and disseminating child abuse photos. Tor is the target of several attacks each year, which cause data breaches and the release of private information. The Tor Network makes advantage of the anonymity function to keep its website and address private while allowing users access to Dark Web services that are concealed from view. Law enforcement will struggle to take them down because their hosting company and location are hidden. The authors have made an effort to thoroughly describe various threat models, including how they operate and how assaults develop.

Cremer et al. [18], mentioned that in 2020, it is predicted that cybercrime would cost the world economy slightly under $1 trillion USD. By 2020, the average cyber insurance claim will have increased to USD 359,000 from USD 145,000 in 2019. The data can be used by cyber insurers to create cyber insurance contracts, calculate cyber insurance rates, and perform various analyses. To better value cyber risks, the datasets might be merged with current pricing algorithms and determinants as well as existing portfolio data from cyber insurers. In 2020, the market for cyber insurance was projected to be worth USD 5.5 billion (Dyson 2020). International trade and the insurance sector both have a sizable knowledge challenge related to cyber risks. This paper provides a contemporary, contextual, and organized summary of the datasets that are currently accessible.

In author in [19], mentioned the following electronic databases were used for the thorough literature search: Academic Search Complete, Criminal Justice Database (ProQuest), EBSCO, Google, JSTOR, and PsychInfo. These investigations used analytical samples ranging from 54 to 5,718 and an average age of 12.4 years. There are various correlations between cyberstalking, abusive online dating, and technological surveillance. A thorough review found that women are more likely than men to experience abuse as a result of online dating. The results show that young people and adolescents need to be better educated on how to have good relationships. Dating, violence, cyber stalking, aggressive and hostile peers, envy, alcohol usage, social media use, time spent online, and poor self-control are all associated with these behaviors.

Yeboah-Ofori et al. [20] review the two dangers that are most predictable in CSC are spear phishing and spyware/ransomware. Predictive analytics give insight into the TTPs, intentions, and motivations of threat actors. The TPR and FPR both have an overall accuracy of 85% according to the projection. For predictive analytics on cyber threats, the method integrates CTI and ML approaches. In order to allow CSC to concentrate on potential system weaknesses, it takes into account both inbound and outbound chains for the vulnerability. With an accuracy of 83%, LR has the highest precision and F-score for malware attacks. With DT and SVM classifiers, DDoS, session hijacking, and spear phishing perform worse. The goal can be to keep APT and command and control presence while changing the software and delivery channels. Through the integration of CTI and ML for threat analysis and forecasting, this research seeks to enhance CSC security.

Since information can influence how a battle turns out, it is crucial to evaluate the harm caused by hackers in between operations as specified in [21]. Using the cyber battle damage assessment framework suggested in this paper, the authors ran an experiment. Mission and attack scenarios were set up for the experiment, and the outcomes of an OMNeT++ simulation were examined. As a result, the mission's performance was 26372 prior to the intrusion. After a cyberattack, the mission's performance was 3697.4, or almost 86% of the harm the attack did. By calculating the threat success rate and host infection rate, damage analysis is performed. In this study, a paradigm is offered for assessing the harm a cyberattack does to a mission. The degree of damage that has occurred can be promptly and quantitatively determined using the damage assessment methodology. The commander may use this information to decide whether to move forward with a mission or not.

Fischer et al. [22], discussed the attacks that cause a distributed denial of service to have an impact on the network resources, computer servers, and website architecture. These attacks are becoming more sophisticated, and they frequently have negative effects on security and the economy. By considering all potential vulnerabilities to software solutions, the security-by-design philosophy seeks to make software solutions as secure as possible. Cybersecurity includes not just safeguarding technology assets but also keeping an eye out in all spheres of the environment for individuals who could constitute a threat to the firm. Designing cyber strategies that establish norms and procedures but are not overly restrictive in the sense that they ignore partner relationships and interpersonal trust presents a challenge.

Zhang et al. [23], informed that many cyber-physical systems (CPSs) are linked to the internet. Cybersecurity tools like message authentication and all-purpose encryption are absent from many CPS systems. To accurately anticipate the system's energy load, a stacked AutoEncoder (AE) model may be used as a regressor. Gas turbine simulation data were gathered and utilised to train the model. For the purpose of learning the advanced features from the input data, a stacked denoising AE (SDAE) was proposed. With an FPR of 0.000006, the suggested model obtained great results. For the purpose of detecting cyberattacks in the context of autonomous vehicles, an LSTM autoencoder architecture was suggested. The AE scored 0.98 on the F1 scale, 0.99 for precision, and 1.0 for recall.

IIT Kharagpur has a state-of-the-art research laboratory called Secured Embedded Architecture Laboratory (SEAL) as mentioned in [24]. IIIT Kanpur is involved in the security of unmanned aerial vehicles (UAVs). Cryptology Research Society of India (CRSI) was set up in 2000 to promote cryptology in India. Cryptography and crypto engineering are the starting points of the overall effort to secure the cyberworld. Fault-injection tools, such as electromagnetic guns, were used to demonstrate that crypto on embedded systems can be attacked. India's cybersecurity industry currently stands at around $10 billion and is likely to grow, according to Forrester. Front-end research on cryptography is becoming more important as India embraces technologies like IoT and CPS to regulate and distribute diverse services.

The Privacy Rights Clearing house reports 7,730 data breaches between 2005 and 2017, accounting for 9,919,228,821 breached records as per [25]. This is the first paper showing that stochastic processes, rather than distributions, should be used to model these factors. The dataset contains 600 hacking breach incidents in the United States between January 1st, 2005 and April 7th, 2017. The hacking breach victims span over 7 industries: businesses-financial and insurance (BSF), retail/merchant including online retail (BSR), educational institutions (EDU) and healthcare providers (MED). The volatility clustering phenomenon exhibited by the log-transformed breach sizes, suggests the use of a GARCH model to model the volatilities in the breach sizes. The result has the qq-plot of the residuals, which shows that the fitting is accurate. This means that the prediction missed some of the extremely large breaches, the prediction of which is left as an open problem. It is observed that the VaR first shows a decreasing trend and then a slightly increasing pattern.

Researchers in [26] informed that in the Dark Web or Dark Net, there are 57% criminal activity and illicit content. According to the United Nations Office on Drugs and Crime, some 2.5 million people are imprisoned in some type of modern slavery. The authors have identified eight key criminal dangers on the Dark Web from the chosen articles, which resolves RQ1. Because Silk Road was run as a Tor hidden service, customers believed their communications there were completely anonymous. Cybercriminals make close to $3.25 billion a year by abusing prominent social media networks. The destination of the connecting server can be determined by implementing hash value analysis at the onion routing's exit node layer. Greater effectiveness is required to reduce possible dangers due to the magnitude of the hidden web. It is more difficult to find criminals on the Dark Web because of its unindexed, fractured, and multi-layered nature.

Wang, Zhu and Sun [27], reviewed that the conceptual model presented in this research offers an integrative and structural perspective to explain how social engineering assaults function. The least resistant people are those that are easily distracted and don't want to debate back. Security is put at risk by inexperience and ignorance. Name-dropping is frequently done out of fear of upsetting superiors. High neurotic individuals are more tense, apprehensive, self-pitying, unstable, and touchy. Victims may help attackers more if they are kind and charitable. Some psychological concepts that have the potential to convince or affect others and work in conjunction with social engineering have been discussed by authors. The purpose of victim exploitation and the effectiveness of social engineering attacks are clarified in this study. Additionally, 16 assault scenarios were provided to show how they could be used. This paper offers a conceptual framework that offers an integrated and structural viewpoint to aid in comprehending the operation of social engineering attacks. Effect mechanisms, human weaknesses, and assault techniques are three key concepts that are examined and explored.

Organizations now pay more than $1.4 million annually on average for social engineering attacks, an increase of 8% from 2017. The study in [28] suggests a new concept for social engineering in cyber security based on the evolution analysis. The suggested concept is compared to typical definitions in the literature using five analysis tables. Based on a thorough literature review, this paper analyzes the conceptual development of social engineering in a systematic manner. Three stages and three strategies make up much of the methodology. Google Scholar is used to finding the pertinent literature first. The cited literature from the references is then looked at in a recursive fashion. Finally, to find difficult-to-find items, Google Scholar and Google's advanced options are used. Social engineering attacks are examples of situations that do not fit specific criteria for SEiCS. These attacks use software flaws instead. The attributes match allows for the analysis and identification of these assaults.

Liu et al. [29] suggested using large-scale unlabelled data sources to pre-train user behaviour sequences, which are composed of logically arranged behaviours, for online fraud detection. High-risk fraud behaviours could be predicted using a pre-trained model. The model must have self-supervised learning methods over intentions in order to be able to identify fraudulent acts. This paper tells the details about the input embeddings, agent tasks, and model training for the suggested UB-PTM technique. The share-private scheme's multi-task learning framework is used to train the model. 0.35 billion transaction pairs make up the pre-training dataset from an online e-commerce platform, of which 0.16 billion, or 46%, are from the same buyer. Results are presented on paper, and the metrics AUC and KS are also used. The AUC is 1.27 percent higher than the IHGAT, and KS is also 1.97 percent higher. On both parameters, the pre-training strategy UB-PTM produces persistent performance gains.

3. FINDING

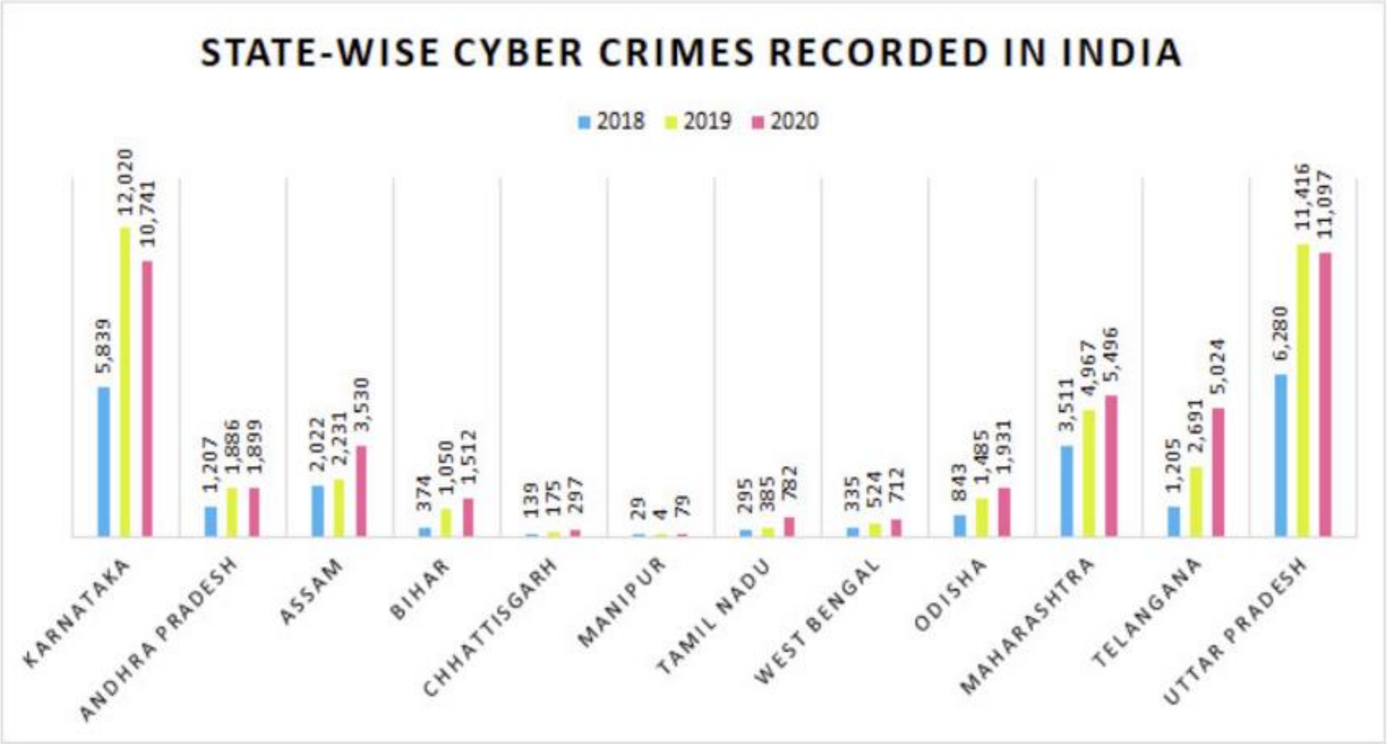

Figure 1 State-wise cyber-crimes report [30]

Figure 1 shows that the number of cybercrime reports is increasing each year in most of the Indian states and thus it is an important part that people should be aware of cyber-crimes happening around them and which can prevent them from being victims of cyber-attacks. This graph shows the rate of distribution of cybercrime around the various states in India from 2018-2020 in which Manipur was found to be the least affected whereas Uttar Pradesh and Karnataka are the most affected with around 11,097 and 10,741 cases as of 2020.

From Figure 2 we can see that 53% of the people have experienced carding and card-related offerings. This shows that card-related frauds are prevailing as compared to other frauds.

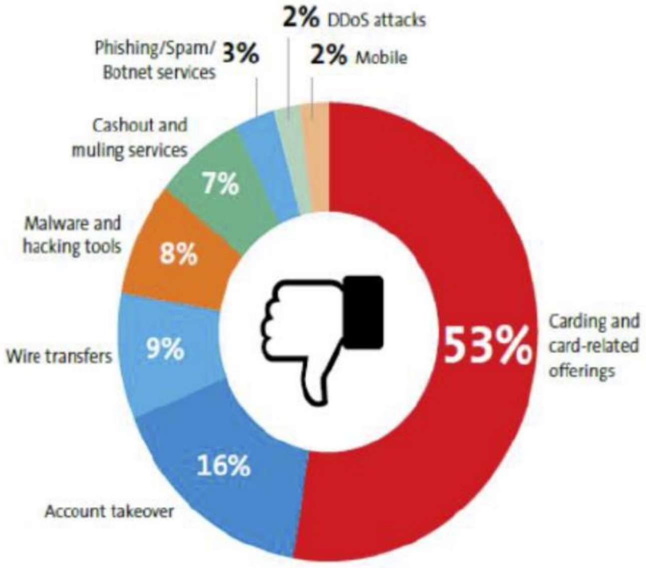

Figure 2. Types of Cyber Scams [31]

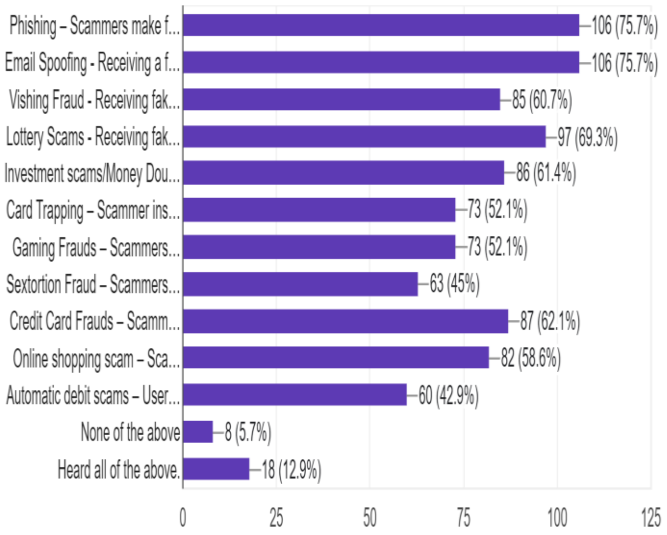

Figure 3. How many cyber scams are you aware of?

One of the major reasons for the growth of cyber scams is the lack of awareness among people about it. The presence of cybercrime cells is not yet known by people. As we can see in Figure 2, credit card frauds are highly on the rise, and according to our survey result, as shown above, only 62.1% of our responders are aware of it and only 42.9% are aware of Automatic debit scams while only 52.1% are aware about card trapping. Automatic debit scams and card trapping are also forms of credit card fraud. The number of scams is increasing day by day and people are still unaware of them.

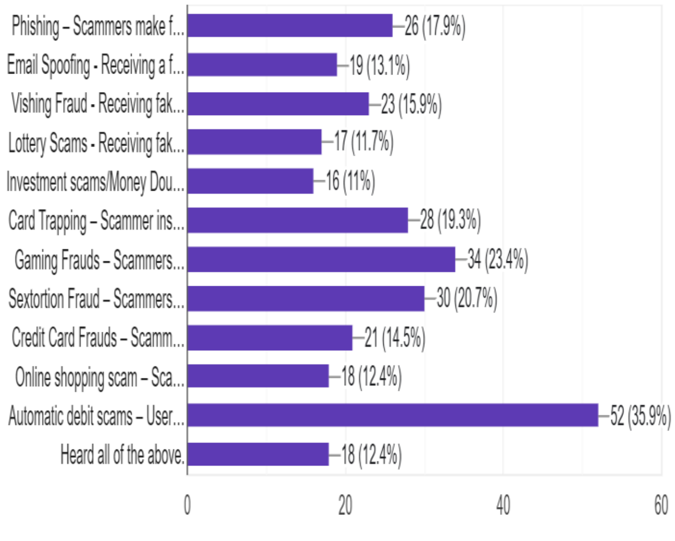

Figure 4. Which cyber scams among these have you never heard of?

According to the survey analysis, 35.9% of people have never heard about automatic debit fraud.

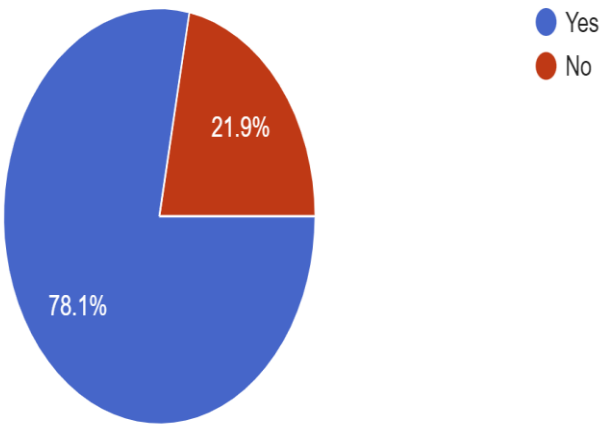

Figure 5. Do you have Antivirus/Firewall Installed on your devices?

According to our survey result, 78.1% of people have an antivirus/firewall installed on their devices, but still, 21.9% of people are unaware of its importance. This makes their device vulnerable to online scams. The devices won't be able to filter out malicious files or scan for viruses, which might corrupt their device.

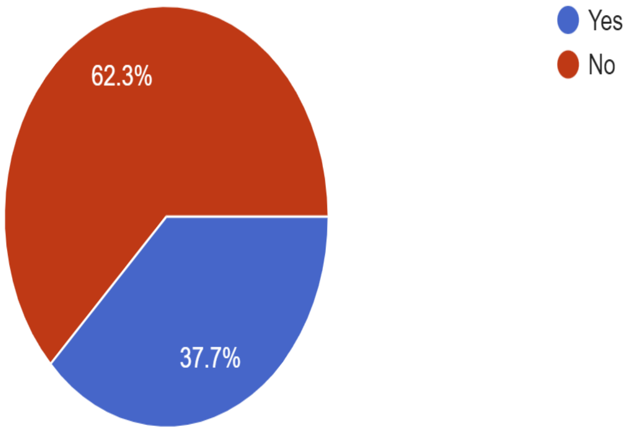

Figure 6. Were you aware of the website "cybercrime.gov.in" and the helpline number "1930" that you need to contact in case of a cybercrime?

When people find themselves becoming a victim of cybercrime, they usually don't know whom to approach and what to do. A lot of people don't even report their incidents to the police. From our survey data, we can know that 62.3% of people are still unaware about the cybercrime website and helpline number, which they can approach in case of experiencing a cybercrime.

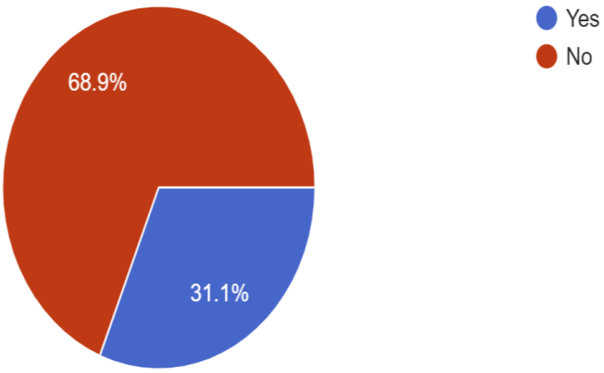

Figure 7. Were your losses ever recovered?

Getting back the money that was lost due to cybercrime becomes difficult and time-consuming at times since tracing back the culprit takes a long time.

Out of 146 people that we surveyed, 61 people faced cyber scams. The total money lost by these people amounted to Rs. 6,49,385.66. Out of 61 people, only 19 people were able to recover some of their lost amounts. The recovered amount totals Rs. 3,16,710.99. The rest of the amount is still unrecovered.

[Note: The stats shown in this paper are completely based on the data received from the survey that was conducted and the data has not been modified under any circumstance.]

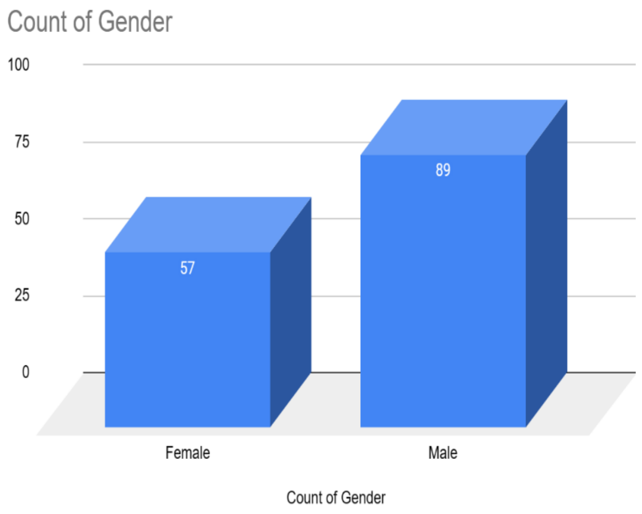

Figure 8. Gender

According to the data received from the survey, it has been observed that 60.9% Male and 39.1% of females had participated in the survey, as shown in Figure 8. The number of males and females who experienced cybercrime is almost equal, thus it cannot be concluded that the probability of one being a victim of a cyber scam is related to his gender.

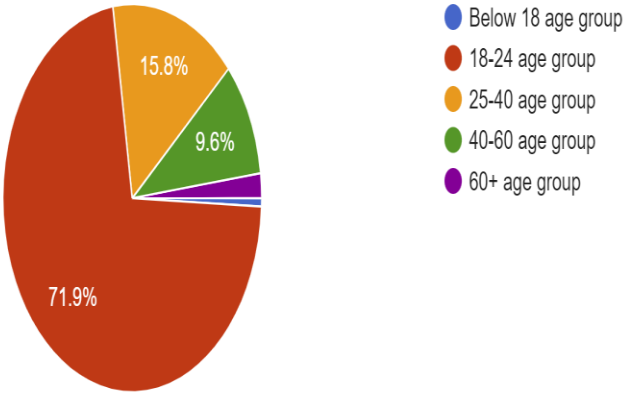

Figure 9. Which age group do you belong to?

From Figure 9 we can see that 71.9% of people who participated in the survey were of ages between 18-24 years, 15.8% were of 25-40 years of age, 9.6% people were of ages between 40-60 years, and 2.1% people were senior citizens of age more than 60 years.

It has also been observed from the survey that the majority of the people who faced cybercrime were youngsters, who are easy to trick and convince. Just as important as it is to earn money, people should also be aware of how to protect themselves against these traps.

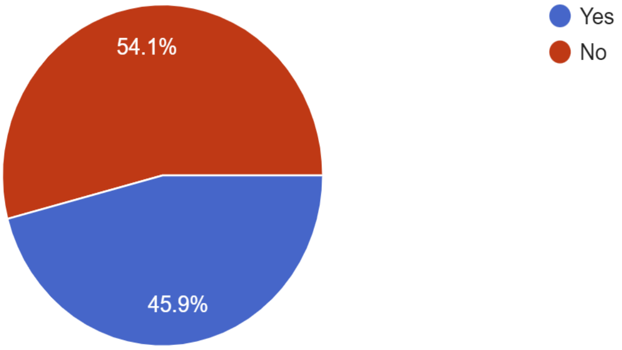

Figure 10. Did you take any steps to catch the culprit?

According to the analysis, 61 people faced cybercrime but only 28 (45.9%, as shown in Figure 10) people took steps to catch the culprit. Only 37.9% of people are aware about the role of cybercrime reporting websites and helpline numbers, which is why the amount recovered is also low. Also, people who are actively reporting are not getting the proper progress due to the limited amount of helplines.

4. CONCLUSION

Despite India ranking 3rd globally for having the highest number of cyber-crimes being reported, people are still not well aware of it. The most common types of cyber scams are related to online transactions. This has caused many bank clients to hesitate when using online banking services. In order to reduce the number of cybercrimes, it is very important for people to be aware about the different types of cybercrimes, the ways people can become a victim of these, and what needs to be done in order to protect themselves. Proper prevention techniques should be taught to everyone irrespective of their age since cybercrime has nothing to do with the age of the user. People should be aware and suspicious of unknown or malicious phone calls, mails, messages, etc. It is also suggested to not provide personal information including bank details on a website if the website is not official. People should also install antivirus or firewalls on their devices. Clicking and opening any link that has been sent by an unauthorized user should be prevented. Bank officials would never ask for OTPs or CVV or passwords over call or mail so this information should not be given to anyone. Prefer to turn off your computer as “always on” makes the computer more susceptible. A firewall protects from unwanted attacks but turning the computer off interrupts and breaks the attacker’s connection. Prefer using strong and different passwords for various websites or accounts rather than using the same. It is advisable to always keep your system and software well-updated. The issue with cyber scams is that it becomes very time-consuming to catch the culprit since those individuals are very hard to recognize and trace. This is one of the reasons for the increasing number of cybercrimes. This study shows that most people who fell victim to these were not able to recover their money. Very few people got back their amount but that was very time-consuming. If people ever find themselves being a victim of such scams, they must be aware about the post-scam steps that they can take which include reporting the incident on the cybercrime reporting portal as well as the helpline number “1930”. The world is heading towards digitalization which makes it even more important to have stronger security since the increasing use of digital media would bring more vulnerabilities resulting in a higher amount of cyber-attacks. Hence the youth must be made well aware of cyber security and more steps towards awareness should be taken not only by individuals but also from society as a whole.

In future work, the research could be done on Network and system vulnerabilities and the effects it could have on the people who faced cybercrime.

REFERENCES

[1] Anisha, "Awareness and strategy to prevent Cybercrimes: An Indian perspective," *INDIAN JOURNAL OF APPLIED RESEARCH,* vol. 7, no. 4, pp. 114-116, 2017.

[2] P. Datta, S. N. Panda, S. Tanwar and R. K. Kaushal, "A Technical Review Report on Cyber Crimes in India," in *2020 International Conference on Emerging Smart Computing and Informatics (ESCI),* Pune, India, 2020.

[3] Z. Yu, Z. Kaplan, Q. Yan and N. Zhang, "Security and Privacy in the Emerging Cyber-Physical World: A Survey," *IEEE Communications Surveys & Tutorials,* vol. 23, pp. 1879-1919, 2021.

[4] J. A. Adejobi, F. Carroll and R. Montasari, "How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society," *SN Computer Science,* vol. 3, 2022.

[5] A. B. Cengiz, G. Kalem and P. S. Boluk, "The Effect of Social Media User Behaviors on Security and Privacy Threats," *IEEE Access,* vol. 10, pp. 57674-57684, 2022.

[6] M.-E. Paté-Cornell and M. A. Kuypers, "A Probabilistic Analysis of Cyber Risks," *IEEE Transactions on Engineering Management,* vol. 70, pp. 3-13, 2023.

[7] W. Duo, M. Zhou and A. Abusorrah, "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges," *IEEE/CAA Journal of Automatica Sinica,* vol. 9, pp. 784-800, 2022.

[8] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq and M. K. Khan, "Comprehensive Review of Cybercrime Detection Techniques," *IEEE Access,* vol. 8, pp. 137293-137311, 2020.

[9] P. Triantafyllopoulou, C. Clark-Hughes and P. E. Langdon, "Social Media and Cyber-Bullying in Autistic Adults," *Journal of Autism and Developmental Disorders,* vol. 52, pp. 4966-4974, 2022.

[10] S. D. Johnson and M. Nikolovska, "The Effect of COVID-19 Restrictions on Routine Activities and Online Crime," *Journal of Quantitative Criminology,* pp. 1-20, 2022.

[11] M. Kaur and M. Saini, "Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions," *Education and Information Technologies,* pp. 1-35, 2022.

[12] A. Kovačević, N. Putnik and O. Tošković, "Factors Related to Cyber Security Behavior," *IEEE Access,* vol. 8, pp. 125140-125148, 2020.

[13] R.-V. Mahmoud, M. Anagnostopoulos and J. M. Pedersen, "Detecting Cyber Attacks through Measurements: Learnings from a Cyber Range," *IEEE Instrumentation & Measurement Magazine,* vol. 25, no. 6, pp. 31-36, 2022.

[14] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman and M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," *IEEE Access,* vol. 10, pp. 39325-39343, 2022.

[15] H. Abroshan, J. Devos, G. Poels and E. Laermans, "Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process," *IEEE Access,* vol. 9, pp. 44928-44949, 2021.

[16] G. Tsakalidis and K. Vergidis, "A Systematic Approach Toward Description and Classification of Cybercrime Incidents," *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* vol. 49, no. 4, pp. 710-729, 2019.

[17] J. Saleem, R. Islam and M. A. Kabir, "The Anonymity of the Dark Web: A Survey," *IEEE Access,* vol. 10, pp. 33628-33660, 2022.

[18] F. Cremer, B. Sheehan, M. Fortmann, A. N. Kia, M. Mullins, F. Murphy and S. Materne, "Cyber risk and cybersecurity: a systematic review of data availability," *Geneva Papers on Risk and Insurance - Issues and Practice,* vol. 47, p. 698–736, 2022.

[19] C. D. Marcum and G. E. Higgins, "A Systematic Review of Cyberstalking Victimization and Offending Behaviors," *American Journal of Criminal Justice,* vol. 46, pp. 882-910, 2021.

[20] A. Yeboah-Ofori, S. Islam, S. W. Lee, Z. U. Shamszaman, K. Muhammad, M. Altaf and M. S. Al-Rakhami, "Cyber Threat Predictive Analytics for

Improving Cyber Supply Chain Security," *IEEE Access*, vol. 9, pp. 94318-94337, 2021.

[21] S. Kim, J. Jang, O.-J. Kwon, J.-Y. Kim and D. Shin, "Study on Cyber Attack Damage Assessment Framework," *IEEE Access*, vol. 10, pp. 59270-59276, 2022.

[22] B. Fischer, D. Meissner, R. Nyuur and D. Sarpong, "Guest Editorial: Cyber-Attacks, Strategic Cyber-Foresight, and Security," *IEEE Transactions on Engineering Management*, vol. 69, no. 6, pp. 3660-3663, 2022.

[23] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen and Y. Xiang, "Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 377-391, 2022.

[24] D. Mukhopadhyay, "Cybersecurity in India," *Communications of the ACM*, vol. 65, no. 11, pp. 98-102, 2022.

[25] M. Xu, K. M. Schweitzer, R. M. Bateman and S. Xu, "Modeling and Predicting Cyber Hacking Breaches," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2856-2871, 2018.

[26] S. Nazah, S. Huda, J. Abawajy and M. M. Hassan, "Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach," *IEEE Access*, vol. 8, pp. 171796-171819, 2020.

[27] Z. Wang, H. Zhu and L. Sun, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," *IEEE Access*, vol. 9, pp. 11895-11910, 2021.

[28] Z. Wang, L. Sun and H. Zhu, "Defining Social Engineering in Cybersecurity," *IEEE Access*, vol. 8, pp. 85094-85115, 2020.

[29] C. Liu, Y. Gao, L. Sun, J. Feng, H. Yang and X. Ao, "User Behavior Pre-training for Online Fraud Detection," in *Association for Computing Machinery*, Washington DC, USA, 2022.

[30] N. Singh, "Cyber Crimes in India Spiked Nearly Nine Times Since 2013, UP Topped Chart in 2020: Data," CNN-News18, New Delhi, 2021.

[31] J. Iqbal and B. M. Beigh, "Cybercrime in India: Trends and Challenges," in *International Journal of Innovations & Advancement in Computer Science, IJIACS*, Joginpally B.R.Engineering College,Hyderabad,India, 2017.

BIOGRAPHIES

Moulik Singh Arora is a B.Tech student majoring in Information Technology at Vellore Institute of Technology, Tamil Nadu, India. His academic pursuits are complemented by a keen interest in cybersecurity, cyberattacks, security and privacy, and ethical hacking. With a strong foundation in IT, Moulik is dedicated to exploring innovative solutions and contributing to the field of cybersecurity through research and practical applications.

Preksha J Dadhania is a dedicated student pursuing a B.Tech degree in Information Technology at Vellore Institute of Technology, Tamil Nadu, India. Her academic journey is driven by a passion for Web Development, cyberattacks, and ethical hacking. Through her studies and research endeavors, Preksha aims to contribute to the advancement of cybersecurity practices and explore innovative solutions in the field.