International Journal of Research in Multidisciplinary Studies (IJRMS)
Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi

Cyber Security and Artificial Intelligence

Anupama Kumari
Bharati Vidyapeeth's
Institute of Computer Application and Management
New Delhi. India
anupamakumari2001@gmail.com

Shweta Nayal
Bhai Parmanand
Institute of Business Studies
New Delhi, India
rsnayal4@gmail.com

Rohit Nayal
Delhi Skill and Entrepreneurship University
New Delhi, India
rsnayal8@gmail.com

Atish Kumar
Vivekananda Institute of Professional Studies
New Delhi, India
atishkumar1807@gmail.com

***Abstract*— The world has seen an extraordinary surge in artificial intelligence (AI) solutions in recent years, which has fundamentally changed how technology functions in our day-to-day lives. These AI systems—which range from predictive analytics to virtual assistants—have ingrained themselves into our digital environment and are reshaping how businesses operate, interact, and make decisions. But despite all of these technologies' great promise, there is one urgent worry: the possibility of personal data leakage. Large-scale data mining of potentially copyrighted materials, like texts, images, and videos, is necessary for AI advancements. Concerns about data privacy breaches and unauthorized access have increased as a result of AI solutions' heavy reliance on data for training and operation. This has emphasized how important it is to use AI's power while protecting the sensitive data that it needs. The quest to strike a balance between the imperative of data protection and AI's amazing capabilities is more important than ever in this context. The research sets out on a critical exploration of the rapidly changing field of technology, where AI-driven solutions have become increasingly prevalent. The goal of the study is to discover how transparent the privacy policies governing browser plug-ins, desktop apps, and browser-only AI solutions are. The most prevalent inquiry is, "How safe is our data?" Cybersecurity is essential in the field of information technology. Information protection has become one of the major concerns these days. When we consider cyber security, the first thing that comes to mind is "cybercrimes," which are becoming worse every day.**

To stop these cybercrimes, numerous governments and organizations are putting various strategies into practice. Many people still have grave concerns about cyber security in spite of these precautions. As technology develops, hacker techniques also become more sophisticated. Fortunately, despite all of these theories, engineers have made significant advancements in threat detection technology. Modern AI cybersecurity systems that are the most sophisticated include machine learning into their threat detection procedures. We have essentially attempted to concentrate on the question of how to enhance cybersecurity in our research. Despite the fact that many people use the terms AI and ML synonymously, there are important distinctions between them in terms of the underlying technologies and application scenarios.

The primary focus of this paper is the difficulties that modern technologies present for cyber security. It also emphasizes the most recent developments in cyber security methods, morality, and fashions that are redefining the field.

Keywords*— *Cyber Security, Cyber Crime, Cyber Ethics, Data, Digital, social media, Government, Phishing, ML Algorithms, Sycamore, Quantum.

I. INTRODUCTION

These days, a man only needs to click a button to send or receive any kind of data, including audio and video files. However, has he ever thought about how securely his data is being sent to the other person without any information leaking? The answer lies in cybersecurity. The most rapidly expanding.

The internet is modern life's infrastructure. The state of modern technology is changing humanity by the application of several state-of-the-art technologies. Nevertheless, we are unable to adequately protect our personal information due to these new technologies, and as a result, cybercrimes are growing every day. A high level of security was necessary in this field because over 60% of all commercial transactions now take place online in order to ensure the best and most transparent transactions. Thus, cybersecurity has become a modern concern. Cybersecurity encompasses many other domains, including cyberspace, and goes beyond data protection in the IT industry. High security is necessary even for the newest technologies, like cloud computing, mobile computing, net banking, and e-commerce. Protecting these technologies has become crucial because they hold some extremely sensitive personal data about people. Increasing cyber security and protecting critical information infrastructures are essential to any nation's security and economic prosperity. Making the Internet safer is now crucial, and this includes safeguarding network users.
To defend oneself against the increasing number of cybercrimes, everyone should undergo cyber security training.

II. Cyber Crime

The term "cyber crime" refers to any malevolent act or other offense involving electronic communications, information systems, the internet, or any combination of these. Any crime involving a network and a framework, or system, is considered cybercrime. The computer might have been used in the commission of the crime, or it might have been the object or target of it. Digital crimes are defined as crimes carried out with the purpose of causing direct or indirect physical or psychological harm to a victim, or intentionally damaging their reputation through the use of modern telecommunications For instance, notice feeds, emails, messages, cell phones, and Web chat rooms. The safety of the nation and the state of its economy are threatened by such crimes. These are some of the most well-known crimes, especially the ones involving child pornography, hacking, and copyright violations. There are more security risks when confidential information is concealed or disclosed, whether legally or not. Because of the tremendous growth of online share trading and electronic commerce (ecommerce), the number of cybercrime incidents has increased dramatically.

III. Cyber Crime in India

Based on the Federal Bureau of Investigation's 2019 United States Internet Crime Complaint Centre (IC3) report, India is ranked third globally among the top 20 countries where cybercrimes occur.

With 93,796 victims of cybercrimes, the United Kingdom led the list, according to the report, which excludes the USA. Canada (3,721) and India (2,901) followed. According to data from the National Crime Records Bureau (NCRB), India registered 27,248 recorded cases of cyberattack in 2018. Telangana recorded 1,205 cyberattack cases at roughly the same time. The National Cyber Crime Reporting Portal of the Central government has been operational for a year now, and 33,152 complaints have been received. As a result, 790 Federal Investigation Reports have been filed. Cybercrime is not the only issue addressed by the IT Act. A few provisions are also found in the Indian Penal Code.

Here are a few instances of cybercrime that have occurred in India:

- E-Mail Bomb: This type of fraud occurs when a lot of emails are sent to a single email address with the goal of flooding the mail server that supports the address and bringing the service to a complete stop.
- Hacking: It is the attempt to take advantage of a private network or PC framework. It means when someone has an illegal access or control over PC security frameworks. It is carried out by hackers with advanced expertise in breaking into security systems.
- Spreading computer viruses: A malicious program that is installed on a client's computer without the client's knowledge and performs malicious actions, erasing data, is known as a PC infection. It can spread via emails, pen drives (secondary storage), multimedia, and the internet.
- **Phishing:** Phishing is a type of cybercrime in which a person posing as an official organization contacts a target or targets via email, phone, or some message, in an effort to deceive them into disclosing private information, including credit card numbers, passwords, bank account information, and personally identifiable information. Subsequently, the data we obtained is utilized to obtain critical records, leading to widespread fraud, identity theft, and monetary loss.
- **Identity theft:** Act of acquiring someone’s financial or their personal information with the sole intent of using that to conduct business or make purchases. To acquire client lists and destroy credit and personal data, it involves breaking into business databases.

IV. Cyber Ethics

Cyberethics is a subfield of computer technology behavior that establishes the standards for acceptable behavior that users must follow when utilizing computer systems. Cyberethics, to put it simply, is the set of moral principles and computer etiquette that users must adhere to. In general, ethics refers to the spread of moral behavior; similarly, cyber ethics refers to the spread of moral behavior that is not harsh or impolite on the internet. Cyberethics establishes guidelines requiring people to use the internet with civility and responsibility. The goal of cyberethics is to safeguard people's moral, economical, and social conduct. Cyberethics encourages users to utilize technology sensibly and safely, as well as to use it responsibly. The behavior that must be adopted when using cyber technology is understood by cyberethics.

The following is a list of a few cyberethics violations:

- **Cyberbullying:** Cyberbullying is a type of bullying in which victims are made fun of for their looks, way of life, preferences, etc. through the use of internet technologies like social media. The majority of victims of this type of cyberethics breach are teenagers, or perhaps better described as children. Cyberbullying can lead to mental health issues and has an impact on people's ethical standards.
- **Hacking:** It is not regarded as a good practice to steal someone's personal or company information without their consent. It is among the most dangerous cyberattacks in terms of data leaks. Sensitive information, such as passwords and bank account details, may be leaked to a third party user who isn't supposed to have access to it.
- **Copywriting:** Taking credit for someone else's work is another instance of a cyberethics violation that needs to be stopped. Never take up another person's words or documents and pass them off as your own.

It causes plagiarism, which is a major issue that is illegal and subject to punishment. Adhering to general cyberethics is always a good idea when utilizing the internet, or really any type of technology.

V. Case Study

Following are the various case studies for cybercrime:-

A. Andhra Pradesh Tax Case

In Andhra Pradesh, the owner of a plastics company was taken into custody. The Vigilance Department took twenty-two crore rupees in cash from his home. They requested information and explanations from the individual in relation to the unaccounted money. To prove the legitimacy of the company, the accused deposited 6,000 vouchers. However, upon careful inspection of the data and vouchers in his PCs, it became evident that every voucher had been created after the raids had taken place. It was discovered that five companies were operating under the same roof, and it was claimed that they were using computerized and fictitious vouchers to display sales data and evade taxes.

B. The NSP Bank Case

In the situation of Bank NSP, the bank management trainee was engaged and preparing for marriage. The pair utilized the business PC and sent and received a lot of emails. After a while, the two split up, and the girl sent emails to the man's overseas clients using phony email addresses she had created under the name "Indian Bar Associations." She used the bank's PC to do this. The man's business lost a lot of business and sued the bank to make up for it. Emails sent through the bank's PC or system were its responsibility, and the bank was accountable for them.

C. Tamil Nadu vs. SuhasKatti Case

This case is related to the yahoo texting group where explicit, libelous, and annoying messages were posted about a woman who had divorced. Additionally, emails were sent to the victim by the accused using an incorrect email account he had opened in the victim's name in order to obtain evidence. After the message was posted, the woman received obnoxious calls from people who thought she was soliciting. The accused was apprehended by the Police in the following few days after they tracked him down in Mumbai, following the victim's February 2004 complaint. The victim's known family friend, the accused, was allegedly interested in getting married to her.

That being said, she married somebody else. After the marriage ended in divorce, the accused got in touch with her again. The accused started the online harassment because of her reluctance to get married to him. Twelve witnesses were questioned by the prosecution, and all of the documents were designated as exhibits. The court determined that the crime was beyond a reasonable doubt and found the accused guilty based on the testimony of the owners of the Cyber Cafe as well as other evidence presented to it. This case is regarded as the first in Tamil Nadu to result in an offender's conviction under section 67 of the Indian Information Technology Act.

D. Online Credit Card Fraud on e-Bay

Rourkela police uncover a Rs. 12.5 lakh internet scam. The accused's "modus operandi" consisted of hacking into the eBay India website and using the credit cardholders' identities to make purchases. One of the two individuals who were arrested and brought before the sub divisional judicial magistrate's court in Rourkela was the BCA student who is believed to be the mastermind, Debasis Pantit. Apprehended alongside him is Rabi Narayan Sahu. In compliance with Sections 66 of the IT Act and 420 and 34 of the Indian Penal Code, a case has been brought against the defendants. Debasis Pandit is accused of breaking into the eBay India website and gathering the private data of roughly 700 credit card users. At that time, he purchased items by using their password.

When it was noticed that few purchases were coming from Rourkela, even though the customers were based in places like Bangalore, Baroda, Jaipur, and even London, eBay authorities were notified of the fraud. The company received complaints from some of its clients and reported the matter to the Rourkela police.

E. NASA 1999 Cyber Attack

An important turning point in the history of cybersecurity was the NASA cyberattack in 1999, which served as a sobering reminder of how susceptible government organizations and vital infrastructure are to malevolent actors in the digital era. This study delves into the details of the NASA cyberattack in 1999, providing insight into its causes, consequences, and lasting lessons for current cybersecurity initiatives. Targeting NASA's Jet Propulsion Laboratory (JPL), the attack took place in April 1999 and was carried out by a group of people, some of whom were teenagers. Despite their relatively young age, the attackers successfully infiltrated NASA's systems, compromising sensitive information related to satellite missions and space exploration projects. The hack made people wonder if the current cybersecurity measures were sufficient.

VI. AI'S APPLICATION IN CYBER SECURITY

Cybersecurity is undoubtedly one of the most challenging issues that AI is best suited to tackle. Machine learning and artificial intelligence (AI) can be used to "keep up with the bad guys," automating threat detection and responding more quickly than traditional software-driven approaches in light of today's constantly changing cyber-attacks and proliferation of devices.

However, cybersecurity poses a few particular difficulties. :

- A vast attack surface
- Organizations may have tens to hundreds of thousands of devices.
- Countless methods of attack
- Significant shortages of qualified security personnel
- Massive amounts of data that transcend human-scale issues

A self-learning AI-based cybersecurity posture management system ought to be able to handle a lot of these problems. Technologies exist to appropriately train a self-learning system, enabling it to gather data from every information system in your company, continuously and autonomously. The information is then scrutinized and utilized to correlate patterns that are found in millions to billions of signals to the attack surface of the enterprise.

As a result, human teams are able to work with new levels of intelligence in a variety of cybersecurity domains, such as:

- **IT Asset Inventory** – It allows for the accurate and comprehensive inventory of all devices, users, and applications with access. Inventory also heavily relies on business criticality measurement and categorization.
- **Threat Exposure** – Since hackers are fashionistas like everyone else, their tastes in fashion fluctuate frequently. AI-based cybersecurity systems can offer current information on national, international, and sector-specific threats to assist in making crucial decisions about which threats to prioritize based on the likelihood that they will be used to attack your company as well as the possibility that they could be used to do so.
- **Controls Effectiveness** – In order to keep a strong security posture, it's critical to comprehend the effects of the different security processes and tools you've implemented. AI can assist in identifying the gaps and strong points in your infosec program.
- **Predicting Breach Risk** – AI-based systems, which consider the inventory of IT assets, can forecast where and how you are most likely to be compromised. Assets, vulnerability to threats, and efficiency of controls. This enables you to organize how tools and resources are allocated to areas of weakness. Prescriptive insights from AI analysis can help you maximize the effectiveness of your company's cyber resilience by assisting you in establishing and refining policies and procedures.
- **Incident response** – Systems that are enabled with artificial intelligence (AI) can provide improved context for security alert prioritization and response, quick incident response, and the identification of root causes to reduce vulnerabilities and stop issues in the future.
- **Explainability** – In order to support human information security teams, it is imperative to be able to effectively convey the analysis and recommendations supplied by AI. Gaining the support of stakeholders from across the entire organization, comprehending the effects of different infosec programs, and giving pertinent information to all parties—security operations, end users, CISOs, auditors, CIOs, CEOs, and boards of directors—are all dependent on this.

VII. Conventional approach to cybersecurity prior to the rise of AI

Traditional cybersecurity mainly depended on signature-based detection systems prior to the development of AI. By comparing the signatures of known threats or malicious code in an incoming traffic database, these systems operated. When a match was found, the system would notify the user and take the necessary measures to block or quarantine the threat. Although this strategy worked well against established threats, it fell short when it came to unidentified and emerging ones. Hackers could simply get around signature-based detection systems by changing the malware's code or producing new versions that weren't already in the database.

Because authorized traffic may be mistakenly identified as malicious if it happens to exhibit characteristics similar to those of a known threat, signature-based detection systems may produce a large number of false positives. This resulted in security analysts devoting a substantial amount of time to the investigation of false positives, potentially depleting available resources.

Manual analysis was also used in traditional cybersecurity. Security alerts and logs would be manually examined by security analysts who would search for trends or clues that might point to a security breach. This lengthy procedure frequently depended on the expertise of security analyst to identify threats.

VIII. How AI differs from traditional approaches

Traditional cybersecurity mainly relied on signature-based detection systems before artificial intelligence (AI) was introduced. By comparing the signatures of known threats or malicious code in an incoming traffic database, these systems operated. When a match was found, the system would notify the user and take the necessary measures to block or quarantine the threat. This strategy worked well against known threats, but it fell short when it came to unidentified and novel threats. Hackers could simply get around signature-based detection systems by changing the malware's code or producing new versions that weren't already in the database.

Signature-based detection systems may produce a large number of false positives because benign traffic may be mistakenly identified as malicious if it happens to exhibit traits similar to well-known threats. Because of this, examining false positives required a large investment of time from security analysts and might be resource-draining. Manual analysis was also used in traditional cybersecurity. Security alerts and logs would be manually examined by security analysts who would search for trends or clues that might point to a security breach. This was a laborious process that frequently depended on the security analyst's knowledge to pinpoint threats.

IX. AI and ML-based threat detection

Numerous ML algorithms are employed to handle massive amounts of constantly evolving data. This means that in cybersecurity, we have more advanced tools at our disposal to identify trends, foresee dangers, and make use of real-time data.

Let's examine these three use cases to gain an understanding:

A. Predictive modelling for malware

A machine can be trained to detect malware through supervised machine learning. It gains knowledge of the specifications of harmful files. After that, it builds a precise model of those files' appearance. This lets it pre-emptively block malware files. It can do this in spite of the fact that it is impossible to account for every possible variation of malware.

A cybersecurity program that has access to current data can make necessary revisions to its model. A program that is driven by machine learning will continuously learn about malicious

files with various specifications. It can pick up knowledge through its own query and input features, from human input, or from other machines. As it gathers more data, reinforcement learning can stop it from creating new, inaccurate models.

B. *Discrepancies lead to the pursuit of threats*

Pattern recognition is at the heart of machine learning. An AI for cybersecurity can identify irregularities in data transmission patterns. The inconsistency may go unnoticed by the AI as a known threat. Yet, the contradictions alone may set off a threat-hunting mindset. The AI can investigate network traffic and anomalies in greater detail thanks to threat-hunting procedures.

It can act if it has more precise information. It is able to modify its threat model to account for the unusual data. It can also shut the door on data that defies patterns. The AI's decision-making will be guided by prior reinforcement. The AI's parameters sometimes let a human user make the final decision.

C. *Reducing false positives*

Seldom does machine-learning-powered cybersecurity software impede regular traffic flow. Software that is based on rules might find that a lot of harmless files are outside of its scope. Its interference may cause the network to operate more slowly. Programs for machine learning do not depend on specific rules. Alternatively, they can make astute choices. This enables them to block harmful threats without any interruptions.

X. Applied Algorithms

Today, artificial intelligence has a big influence on the world. Machine learning systems are able to learn from test data and carry out intelligent tasks because they are producing large volumes of data from various applications. three different angles on AI-driven security: the data sources being used for analytics, the machine learning techniques being employed, and the desired outcomes. Machine learning is an area of artificial intelligence that focuses on creating apps that learn from data and gradually increase the accuracy of their predictions without the need for manual coding. Applications that use past experience to improve their decision-making or predictive accuracy over time are referred to as machine learning applications.

The process of classifying involves breaking down the dependent variable into smaller groups and then using that information to forecast a class for the input data. Supervised Machine Learning includes it. Because classification algorithms are so good at distinguishing between normal and abnormal patterns in data based on prior experience, they are frequently used in artificial intelligence applications. The Random Forest and Decision Tree algorithms, for instance, are highly accurate and can be used to classify normal and abnormal data with ease in applications such as spam filtering and network intrusion detection.

A. *Random Forest*

Based on decision trees, the Random Forest Machine Learning Algorithm. To make predictions, a number of Decision Trees are combined and put to use. With a random subset of data, these trees function.

$$\text{Accuracy} = \frac{\text{Samples correctly classified in test data}}{\text{Number of samples in test data}}$$

B. *K-means Algorithms*

K-means algorithms are an unsupervised machine learning technique that classify objects into clusters based on their distance from one another. It's a well-liked machine learning algorithm. The K-means algorithm groups data based on similarities found in the dataset. Measure distance or similarity is crucial in grouping observations into homogeneous groups. where the variable k denotes the number of groups.

$$J = \sum_{n=1}^{N} \sum_{k=1}^{K} r_{nk} \, ||\boldsymbol{x}_n - \boldsymbol{m}_n||^2$$

C. *Decision Tree*

The Decision Tree Approach uses a tree-like model to interpret the data by classifying it according to a set of rules. Duplicate features can be automatically excluded from these trees. The process of learning decision trees involves several stages, including feature selection, tree generation, and tree pruning. During the training phase, this model independently determines which features are the most appropriate and then produces child nodes from the root node.

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (fi - yi)^2$$

where yi represents the datapoint's actual value. N is the total number of data points, and i, fi are the values the model returned. The distance of each node from the estimated actual value is calculated using this formula, which aids in determining which branch is best for your forest. Here, yi is the value of the data point you are interested in, and fi is the decision tree's return value.

XI. Exploring Sycamore: Google's Quantum Computing System

As the amount of data grows daily, it becomes more and more difficult to manage such a large dataset, which slows down computation and puts data security at risk. This is where quantum computing comes into play, as it simultaneously interferes with bits to speed up computation. A two-dimensional array called "Sycamore" consists of 54 transmon qubits arranged in a rectangular lattice; each qubit is tunably coupled to its four closest neighbors. By employing the surface code for error correction, the connectivity was selected to be forward-compatible. A significant advancement in systems engineering for this device is its ability to perform high-fidelity single- and two-qubit operations, both independently and in the context of a realistic computation involving multiple qubits performing gate operations simultaneously.

Sycamore, Google's quantum computer, has reached this significant accomplishment. Google showed that Sycamore, in partnership with NASA and Oak Ridge National Laboratory, could calculate in a matter of seconds what would take thousands of years for the biggest and most sophisticated supercomputers. This accomplishment is regarded as a quantum computing breakthrough.

Random quantum circuits were run on both conventional supercomputers and quantum processors as part of the test. Without a quantum processor, it is difficult to extract information from a random quantum circuit. According to theory, even on the biggest supercomputer conceivable, tasks larger than a particular size might not be able to be processed. The Sycamore quantum computer developed by Google is incredibly fast. Its computational speed significantly surpasses that of conventional supercomputers. A particular task that would have taken the Frontier, the most powerful supercomputer in the world, over 47 years to finish, was finished by Sycamore in a matter of seconds. This is because of the special characteristics of quantum computing, whereby quantum bits, or qubits, can simultaneously represent multiple states in contrast to classical bits, which can only represent a 0 or a 1. This makes it possible for quantum computers to process many possibilities at once. In quantum computing, qubits, also known as quantum bits, are the basic building blocks of information. Because of a feature called superposition, qubits can represent both states simultaneously, in contrast to classical bits, which can only be 0 or 1. Because of this, quantum computers can process a large number of possibilities simultaneously, which results in quicker computation times for certain tasks.

Google uses 53 qubits to power its Sycamore quantum computer. However, there are a total of 70 functional qubits in Google's most recent system. Sycamore can complete complicated calculations far more quickly than conventional computers thanks to its large qubit count. One example is collaborative research from IBM and UC Berkeley published last month, which demonstrated that quantum systems can perform better than traditional counterparts even in their still-experimental forms. On IBM's 127-qubit Quantum "Eagle" processor, scientists from both fields performed calculations for complex physical simulation workloads, even in the absence of the fault-tolerant quantum circuits that are required (and for which processors are currently unprepared) to reduce the noise that can impact qubits and classical systems. In the research report, the researchers stated, "We report experiments on a noisy 127-qubit processor and demonstrate the measurement of accurate expectation values for circuit volumes at a scale beyond brute-force classical computation." We contend that this shows how useful quantum computing can be in an age before fault tolerance.

Quantum computing is not just an upgrade; it’s a complete paradigm shift. Unlike traditional binary systems where data is either a ‘0’ or a ‘1’, quantum computers use quantum bits or qubits that can be both ‘0’ and ‘1’ at the same time. This superposition allows quantum computers to perform complex calculations at mind-boggling speeds.

Sycamore performed calculations that would have taken the Frontier, the most powerful supercomputer in the world, seconds to complete. Quantum computing improves combinatoric processing in AI, which is useful for tasks like fraud detection and facial recognition. Quantum algorithms in finance enable faster calculations when pricing complex assets. Quantum-inspired algorithms are used in complex manufacturing to enhance operational procedures and pinpoint the root causes of product failure.

Our mission is to construct one million physical qubits that cooperate within a room-sized error-corrected quantum computer in order to accomplish this goal. Compared to today's modest systems with fewer than 100 qubits, that is a significant leap. In order to get there, we must construct the first "quantum transistor" in history, which consists of two error-corrected "logical qubits" working together to perform quantum operations, and then we must figure out how to tile hundreds or thousands of these qubits to create an error-corrected quantum computer. Because of this, it might take years. In the research report, the researchers stated, "We report experiments on a noisy 127-qubit processor and demonstrate the measurement of accurate expectation values for circuit volumes at a scale beyond brute-force classical computation." We contend that this shows how useful quantum computing can be in an age before fault tolerance.

XII. CONCLUSION

Artificial Intelligence is transforming our world. Machine learning can occasionally transform AI cybersecurity by improving threat detection. Privacy on computers has become a broad and important topic due to the world's increasing interconnectedness and the use of networks for essential transactions. Cybercrime and information security continue to take different turns with each passing year. Protecting their infrastructure from new platforms and threats, in addition to emerging technologies, presents challenges for organizations. These difficulties include the requirement for fresh platforms and intelligence to stay abreast of the most recent technological advancements. We should try our hardest to lessen cybercrimes even though there isn't a foolproof solution to stop them, so that we can keep using the internet safely and securely.

“Stay vigilant, be smart, and you'll be just fine
In this cyber world, where hackers often dine.”

REFERENCES

[1] https://www.researchgate.net/publication/335322600_Cyber_Security
[2] https://medium.com/capital-one-tech/random-forest-algorithm-for-machine-learning-c4b2c8cc9feb
[3] https://lawdocs.in/blog/cyber-offences-under-the-indian-penal-code-1860
[4] https://www.researchgate.net/publication/338419380_Cyber_Security_Threats_and_Vulnerabilities_A_Systematic_Mapping_Study
[5] https://ieeexplore.ieee.org/document/10009154
[6] https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf
[7] https://onlinedegrees.sandiego.edu/top-cyber-security-threats/