10.48047/jocaaa.2024.33.02.30

Generous Cybercrime in the Digital Era: A Criminological Insight

Mr. NAVEEN
Assistant Professor, Department of Computer Science and Engineering, Dronacharya College of Engineering, Gurugram, Haryana
naveen.rathi@ggnindia.dronacharya.info

MS. KAJOL KHATURIA
Assistant Professor, Department of Computer Science and Engineering, Dronacharya Group of Institutions, Greater Noida, Uttar Pradesh
kajol.kathuria@gnindia.dronacharya.info

Abstract

The research proposal focused on the nature, types, theories, legislative approach, judicial trends, survey reports, and human rights aspects of cybercrimes. The author completed an Advance Certificate in Cyber Forensics, Cyber Crimes, Cyber Security & Cyber Law from IFS Education Department, Pune, in July 2017. The paper expanded to include cybercrimes, cyber criminology, cyber space, right to privacy, cyber laws, case law, cyber forensics, cyber security framework, and cyber risk management. The paper highlights the need for a special area called Cyber Criminology in legal education, covering cyber laws, cyber space, criminal behavior in cyberspace, motivational factors, and different types of cybercrimes, judicial cases, cyber forensics, tools used, cyber risk management, and cyber security framework. The research aims to demonstrate the vastness of cybercrime and the need for a comprehensive educational course covering all related aspects to create well-trained professionals in the field.

Keywords: Cybercrimes, Cyber security, survey reports, cyber forensics, broad vision.

Introduction

Information technology has both positive and negative impacts on human and organizational performance. While it can improve performance, it can also pose significant threats to individuals, organizations, and society if used maliciously. Cybercrimes involve computer networks and can be used as tools for committing crimes or as targets for illegal digital activities. Cybercriminals are well-versed in computer technologies and use advanced technologies to commit crimes [1].

In the network age, online communication has become a norm, and the United Nations General Assembly passed resolutions on cyber security in 2010 and 2019 to prevent illegal use of ICT. Governments must implement measures to safeguard internet users while introducing laws or regulations to prevent the misuse of Information and Communication Technology. The Information Technology Act, 2000 in India is the first legislation relating to information technology and crimes related to technology [2].

The United Nations Commission of Human Rights has highlighted the negative impact of misuse of information technology on privacy, highlighting the need for an interdisciplinary approach involving law, criminology, forensics, and technology. This approach should cover all aspects of cybercrime, from the evolution of the internet to the concept of cyberspace, classification, types of cybercrimes, right to privacy in cyberspace, criminal liability in cyberspace, cyber laws, cyber forensics, cybersecurity issues with data protection, cloud computing, and the use of artificial intelligence in cyber security [3].

10.48047/jocaaa.2024.33.02.30

The research aims to understand cyber criminology, study the issues and challenges of cybercrimes, identify potential threats in a networked age, study the nature, scope, classification, and types of cybercrimes, and explore the right to privacy, accountability, and theories of criminal behavior in cyberspace. The study will also analyze existing national and international laws, national policies, court roles, and potential cyber security measures to control cybercrime [4].

The research hypothesizes that the current legislative approach in India is inadequate to prevent cybercrimes, and whether courts can tackle cybercrime cases in the current criminal justice system. It also explores the effectiveness of effective and sustainable cybercrime risk management in curbing cybercrime [5].

Fig.-1 Aims of Cyber Security Structure

The research is conducted over seven years, focusing on issues related to cybercrimes, nature, types, and theories of criminal behavior in cyberspace. The study aims to bring together all issues and challenges related to cybercrime, including its characteristics, nature, history, classification, laws, cyber forensics, cybersecurity management, and cyber criminology as a separate academic discipline. The research methodology is based on both qualitative and doctrinal research, analyzing books, articles, research papers, and journals [6].

This research aims to study the criminological perspective of cybercrimes in a network age and explore the issues and challenges faced. The research will examine the concept of cybercrime, its history, types, factors responsible for cybercrimes, criminological behavior in cyberspace, laws related to cybercrimes, the concept of cyberspace, right to privacy in cyberspace, different theories of crime in cyber space, cyber forensics, cyber laws and cases, cyber security, and data protection [7]. The literature review will examine whether existing literature has comprehensively covered all topics related to cybercrimes. Books and journal articles examined include Justice Yatindra Singh's "Cyber Laws," Nandan Kamath's "Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000,"

10.48047/jocaaa.2024.33.02.30

Vakul Sharma's "Information Technology; Law and Practice: Cyber Laws and Laws Relating to E-Commerce," Rodney D. Ryder's "Guide to Cyber Laws (Information Technology Act, 2000, Ecommerce, Data Protection and the Internet), and N.S. Nappinai's "Technology Laws Decoded." The research aims to provide a comprehensive understanding of various technology laws in India, international conventions relating to cybercrime, and the governance of cyber space [8].

The book Cyber and E-commerce Laws with Information Technology Act, 2000, by Parag Diwan and Shammi Kapoor covers topics such as information theft, data protection, copyright protection, E-commerce laws, cybercrimes, and individual rights and remedies. Dr.Jyoti Rattan and Dr. Vijay Rattan discuss the evolution of the internet, network security, and cybercrimes. They cover topics such as E-commerce, E-Governance, ERecord, and E-Contract, cryptography, digital signatures, encryption techniques, certifying authorities, subscribers, regulators, E-evidence, consumers, ISPs, intellectual property rights, privacy of online data, freedom of expression, and speech in online forums [9].

Cyber Law: Indian & International Perspectives on key topics includes data security, E-commerce, cloud computing, and cybercrimes. Authors like Aparna Viswanathan cover areas like cyber terrorism, cybercrimes, cloud computing, electronic signatures, encryption, decryption, data security and privacy, intellectual property in internet, and statutory rules and guidelines in India and internationally [10].

In Cyber Law 3.0, Pavan Duggal explains various sections of the Information Technology Act, 2000 and the amendment Act of 2008, including digital signatures, electronic governance, electronic records, regulation of certifying authorities, electronic signature certificates, duties of subscribers, penalties, compensation and adjudication, cyber appellate tribunal, various cyber offenses, and intermediaries are not liable in certain cases [11].

Seth, a cyber lawyer, highlights the emergence of the E-information society and the jurisdiction in the transnational cyberworld. She discusses issues related to cyberspace, such as intellectual property rights, data privacy, cyber contraventions, and cybercrimes. In various books, various authors discuss the legal issues surrounding cybercrimes, including Vivek Sood's "Cybercrimes, Electronic Evidence and Investigation: Legal Issues," Dr. M. Dasgupta's "Cybercrimes in India: A Comparative Study," V.D. Dudeja's "Cyber-crimes and the Law," R.K. Chaubey's "Kamal's an Introduction to Cyber-crimes and Cyber Law," and others [12].

In "Cyber Crimes," the authors trace the evolution of criminal law, criminal justice system, and the concept of cybercrimes. They also examine emerging trends like dark web, net neutrality, cloud computing, cyber infractions, and intellectual property issues in technology. In "Legal Dimensions of Cyber Space," S.K. Verma and Raman Mittal discuss the concepts of the cyber world, the history, development, merits, and demerits of the internet, and the indispensable role of computers and the internet in leading to crimes in the cyber world. In "Trademarks & the emerging concepts of Cyber Property Rights," Unni V.K. discusses trademarks, domain names, and cybersquatting, while also discussing the role of WIPO in domain management and uniform dispute resolution policy. In conclusion, these books provide valuable insights into the legal issues surrounding cybercrimes, the importance of effective cooperation between law

10.48047/jocaaa.2024.33.02.30

enforcement agencies, and the legal implications of cybercrimes [13].

Trademarks and the Emerging Concepts of Cyber Property Rights is a comprehensive book that covers various aspects of cyber security, including domain disputes, trademark ownership, and protection of non-proprietary pharmaceutical names in the DNS. The Indian reprint of Butterworths Data Security Law & Practice provides an overview of data security laws in the United Kingdom, covering the development of data security law, government reforms, price privacy, security principles, confidentiality, privacy relating to technology, communication privacy, personal data, and general rules of data protection. The International Encyclopaedia of Laws in Cyber Law is divided into three volumes, covering national monographs from Australia, Cyprus, Denmark, Hellas, Hong Kong, Ireland, Japan, Mexico, Portugal, South Africa, Spain, and the United Kingdom. The book is divided into seven parts, covering various aspects such as intellectual property protection, contract law principles, electronic transactions, non-contractual liability, privacy protection, and computer-related crime [14].

In their article "Inside of Cybercrimes and Information Security-Threats and Solutions," Maghu et al. discuss the threats of cybercrimes in daily life, such as banking transactions and shopping, and provide solutions for protecting against cyberattacks. Justice Michael Kirby discusses the need for review of existing regulations and standards, as well as the OECD guidelines on privacy. He emphasizes the importance of national governments in defending individual privacy as a fundamental right and calls for the development of principles on information privacy in harmony with internet development. The article "The Criminalization of True Anonymity in Cyberspace" by Du Pont explores the issue of whether federal or state governments can impose restrictions on anonymity in cyberspace without violating the First Amendment. The US Supreme Court has not directly addressed this issue, but Du Pont concludes that restricted legislation related to true anonymity would not be a violation of the First Amendment. Diamond and Bachmann provide an overview of cyber criminology study, highlighting the challenges faced by researchers and suggesting solutions. They also discuss the global issue of cybercrime, which costs individuals and organizations around 180 billion Euros annually. They argue that advanced computer technology is the only way to combat cybercrime [15].

Saroha discusses the disturbing nature of cybercrime, stating that with technological growth, computers have become essential for sharing information and data, leading to a new type of crime using computers. She identifies the personality traits of cyber criminals under four heads: technical know-how, personal traits, social characteristics, and motivating factors. Barman examines the legal implications of cybercrimes on social networking websites, highlighting the vulnerability of social media to modern technology-related crimes. K. Jaishankar, the founding father of cyber criminology, explains that academics and criminologists initially struggled to understand cybercrimes. He argues that cyber criminology involves multidisciplinary fields like sociology, psychology, victimology, information technology, and computer science. Jaishankar believes that there is a need for a comprehensive educational course that includes cyber criminology, law, and forensics to take cyber criminology to the next level. Sun et al. discuss the importance of data security and privacy in cloud computing, highlighting the challenges in protecting data integrity, confidentiality, availability, and privacy. They argue that organizations should not transfer their data to the cloud without developing trust with cloud service providers. Shweta Chhetri discusses the ease of transmitting information globally in the 21st century,

10.48047/jocaaa.2024.33.02.30

emphasizing the need for strong legislation and separate cyber security laws in India. Madarie analyzes the motivations of hackers and their motivation to hack, finding that most hackers have curiosity to bypass security systems and aversion to traditional values. King examines the constitutionality of cyber-bullying laws, focusing on the case of Megan, who was using Myspace and resulting in clinical depression and suicide. She emphasizes the need for proper laws to protect teenagers from cyberbullying, despite the delicate issue of online speech regulation in constitution law [16].

Research Methodology

The rapid growth of technology and social media has led to increased reliance on unsecured networks and connected devices, making it easier for cybercriminals to access and cause damage. The pandemic has also led to a rise in work from home, resulting in more organizations adopting cloud computing. However, using cloud computing without proper security features is also dangerous, as 2021 has seen numerous data breaches and ransomware attacks. Cyber security risks involve the loss of sensitive information and critical data due to cyber-attacks on an organization. There are three components of cyber security risks: threat, vulnerability, and consequences. The first component includes social engineering attacks, which can result from a weak technology management system [17].

Fig.-2 Three critical elements of Cyber Security

Types of cyber-attacks include network attacks, wireless security attacks, malware attacks, virus attacks, worms, and social engineering attacks. With the development of technology, businesses have begun using cloud-based services for keeping critical data, which can pose cyber security risks. Cloud platforms can expose sensitive corporate or personal data, and modern encryption techniques can protect data integrity. API weaknesses, particularly in cloud services, can compromise the privacy of cloud orchestration, administration, provisioning, and monitoring. Malicious insiders may also attempt to leak data or tamper with cloud orchestration for personal gain. Therefore, organizations must be cautious when using cloud computing without proper security features [18].

10.48047/jocaaa.2024.33.02.30

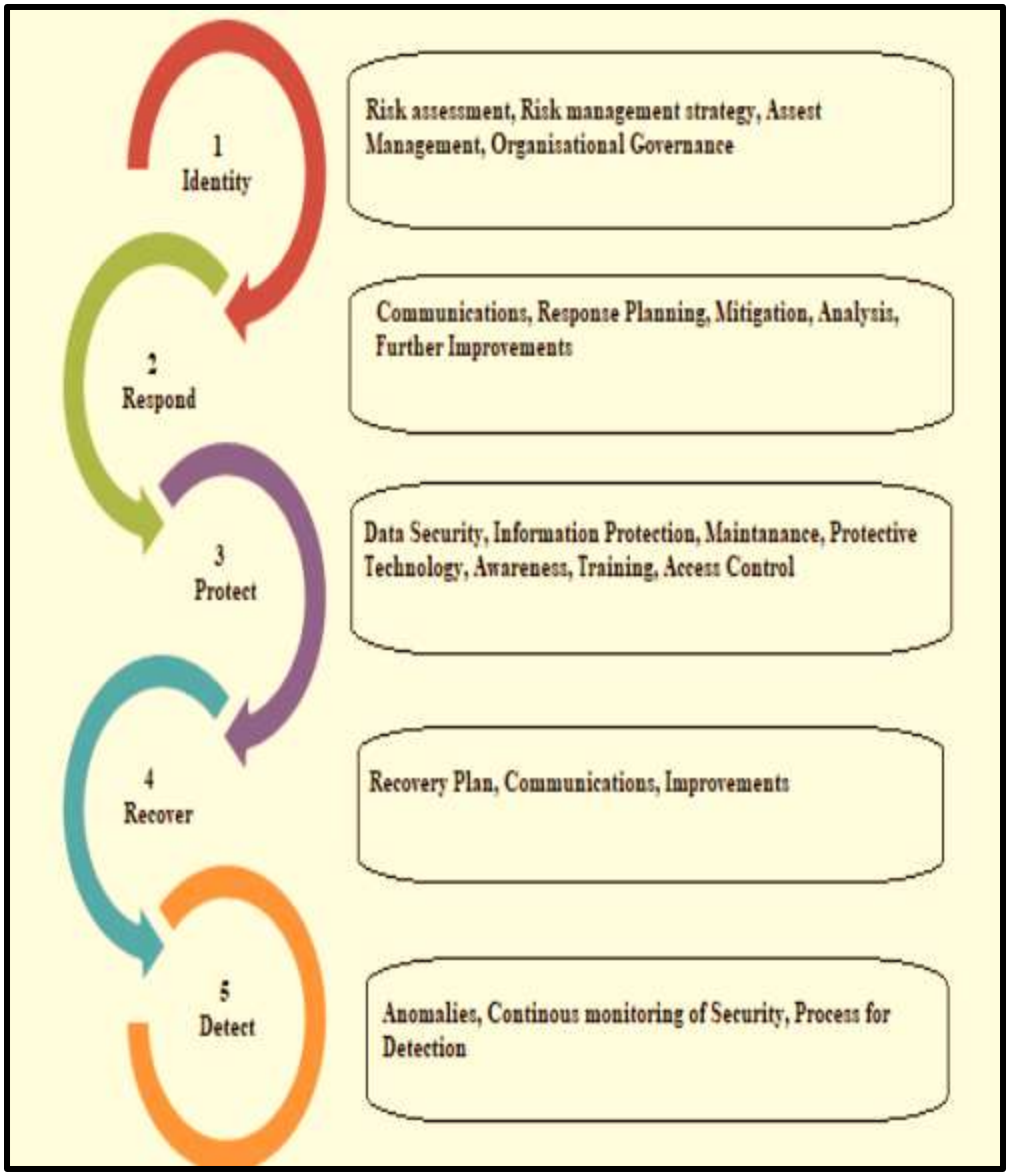

Fig.-3 Process flow

Fig.-4 Seven Steps to Build a Cyber Security programme

10.48047/jocaaa.2024.33.02.30

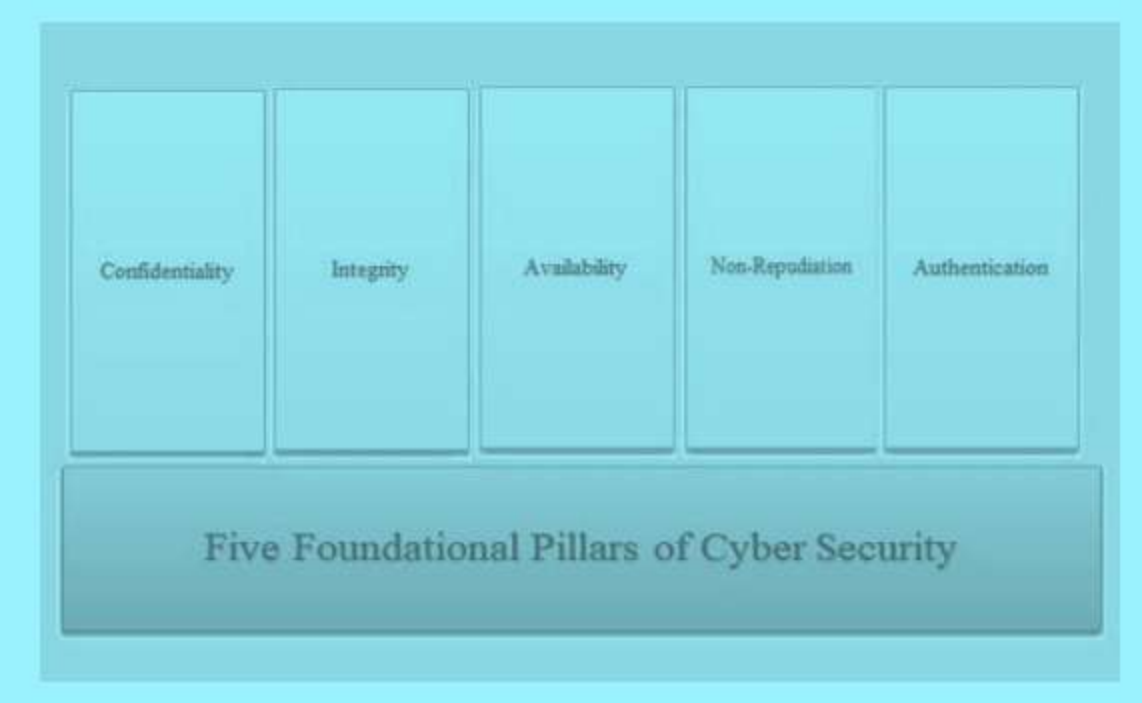

Fig.-5 Five foundational pillars of Cyber Security

Cloud computing technologies, such as virtualization and cloud orchestration, can be exploited by hackers to inflict severe harm on users. Hackers can take over virtual machines and even the host itself if the hypervisor has flaws. Lock-in providers often make their clients dependent on their services with high switching costs, making many feel locked in. Good cryptographic techniques can safeguard stored data, but not all encryption methods are adequate. Cloud services are not adequately protected against one another, allowing attackers to take advantage of weaknesses in any one cloud service to gain unauthorized access to legitimate customers' data. Cyber threats against cloud computing aim to gain access to user data and block users from accessing services, causing significant harm to users and undermining public faith in the security of cloud services. Ten most common attacks on cloud platforms include cloud malware injection attacks, misuse of cloud services, and denial-of-service attacks. Malware injection attacks aim to gain access to user information stored in the cloud, while misuse attacks exploit low-cost cloud services to launch distributed denial-of-service (DDoS) and brute-force attacks against target individuals, businesses, and other cloud service providers. Denial-of-service attacks are designed to overburden a system and render its services inaccessible to users, causing widespread damage and loss of many users [19].

Cyberattacks on cloud systems can be more damaging due to the sluggishness of the cloud infrastructure and the lack of security measures in place. Side channel attacks, wrapping attacks, man-in-the-middle attacks, insider attacks, account or service hijacking, advanced persistent threats (APTs), and new cyberattacks like Meltdown and Spectre can all pose significant threats to cloud computing. Side channel attacks target cryptographic algorithms, while wrapping attacks exploit XML signatures to tamper with user information. Man-in-the-cloud attacks exploit synchronization token system vulnerabilities, allowing attackers to monitor and reconfigure cloud services. Insider attacks involve valid users intentionally breaching security

10.48047/jocaaa.2024.33.02.30

policies, while insider attacks involve attackers taking on the roles of cloud providers or client organizations. Account or service hijacking can be achieved through various methods, such as fishing, spyware, and cookie poisoning. Advanced persistent threats allow attackers to gain confidential data or abuse cloud services without detection, making them more adept at circumventing security mechanisms. The rapid adoption of digital technology in both private and public sectors has led to a lack of proper backend cyber security infrastructure, placing a significant amount of data at risk. India, as the world's second-largest consumer of smart gadgets and one of the world's largest internet users, continues to be a vulnerable country for national and international cyber-attacks due to its outdated infrastructure [20].

Social engineering and phishing attacks are prevalent threats that involve duping and convincing individuals to perform activities or provide information without realizing the repercussions. The rise of e-commerce has increased the number of such attacks. As governments and economies adjust to the new normal, technology inventors are working to develop solutions to help businesses maintain operations and flourish. India, the second-largest user of new devices in the world, remains an easy target for both domestic and international cyberattacks due to its outdated technology and weak security measures.

Cloud computing offers flexibility to cyber criminals, but it exposes vulnerabilities, making it difficult for organizations to use cyber forensics. Vulnerabilities in APIs can jeopardize the security of cloud management, and robust controls over APIs can help prevent breaches. Common cyberattacks on cloud computing include malware injection, abusing cloud services, denial of service attacks, side-channel attacks, wrapping attacks, insider attacks, user account hijacking, spectre, and meltdown.

Cyber security is essential to protect sensitive information, such as national security, financial records, and personal information. However, people have limited understanding of cyber security and its prevention, with antivirus and malware protection software being the most common. The fragmented and unorganized cybersecurity infrastructure and lack of effective regulations impede detection and prosecution of cyber thieves. Cloud vulnerability is a serious concern, with larger companies investing heavily in security but smaller businesses and organizations hesitant to adopt it.

Cloud services (CS) have evolved significantly, making it crucial for providers to follow industry best practices to ensure user data safety. To increase cybersecurity, providers should increase the effectiveness of their security protocols, implement strong authentication, allocate role-based rights to administrators, and safeguard information through encryption at every phase of data storage and transmission. Using encryption algorithms like salt and hashes and offering data backup services can help protect against cyberattacks.

To identify intrusions, cloud providers should assemble an intrusion detection system (IDS) that monitors the network and alerts when insiders exhibit unusual behavior. Developers should ensure that only secure APIs are used for accessing application data, reducing the range of IP addresses available or restricting access to business networks or virtual private networks (VPNs).

To protect cloud services, developers should minimize event handler permissions and restrict

10.48047/jocaaa.2024.33.02.30

security decisions to only trusted CS. By understanding how cybercriminals attack cloud computing, developers can better protect their products. Apriorit, with its expertise in cloud engineering, virtualization, and cybersecurity, can help enhance the security of their cloud-based solutions. Mariana Pereira, head of Darktrace, warned about the potential threat posed by virtual assistants during an AI and Machine Learning conference at the University of California, Berkeley. She expressed concern about the potential for AI-powered hackers to gain access to sensitive data, such as malware that could infiltrate messages or send malicious emails. The increasing dependency on cloud computing presents unique challenges for EU policy, particularly in areas of cybercrime and privacy. Cloud computing contributes to the increase of cross-border data flows, creating legal issues related to data security, jurisdiction and accountability, data transfer regulations, and the activity of EU authorities. Risks related to cloud computing are an aggravation of established information security issues, with the risk experienced by individuals adopting cloud services being the most significant. Data security and secrecy are often negotiated at the cost of individual rights, and the idea that cloud computing is breaking away from the 40-year-old legal norm for foreign transmitting data is perhaps the most damaging aspect of cloud computing.

The difficulty of maintaining privacy in a cloud environment is grossly underestimated, and data protection regulations are often low on the priority list in European fora concerned with cybercrime. The issue of protection of personal data and privacy is further complicated by extraordinary measures adopted in the name of security and counterterrorism, such as the Patriot Act and the Foreign Intelligence Surveillance Amendment Act (FISAA) of 2008. Standardizing what constitutes personal information at the EU level would help address these issues more consistently. Cloud computing is not a truly new technology but does lead to the improvement in cross-border data flow, presenting unique challenges to EU policies, particularly in privacy and cybercrime. Cloud computing is a technology that distributes resources across data centres, providing services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS). However, it lacks traditional security features and on-site software, making it vulnerable. Organizations and institutions should develop cyber security policies, create awareness among users, install spam filters, firewalls, antivirus, and anti-malware software, perform vulnerability assessments, have a software program for preventing data loss, and prepare guidelines for accessing the internet and using the cloud platform.

Artificial Intelligence (AI) has gained interest in cybersecurity due to its ability to detect unexpected cyberspace intrusions quickly and efficiently. Conventional security methods rely on virus protection, firewalls, and other technologies to identify and mitigate web-based security risks. AI relies on technological breakthroughs like Machine Learning to identify and prevent cyberattacks. AI can be used to prevent cyberattacks by simulating how an attacker would think and behave in terms of breaking the security code. For example, if a webpage receives less traffic or contains highly confidential information, AI can manage the security of high-profile sites. However, it is essential to consider the specific needs and priorities of different websites and platforms when implementing AI-based tools. In conclusion, while cloud computing offers numerous benefits, organizations and institutions must also take responsibility for their security measures and implement robust security measures.

10.48047/jocaaa.2024.33.02.30

Analysis and Overview of Cyber Laws

The Information Technology Act, 2000 was drafted in India in 1999 following the Model Law on electronic commerce adopted by the UNCITRAL in 1996. The Act aimed to facilitate electronic governance and commerce in India, create civil and criminal liabilities for crimes related to electronic mediums, and ensure legal recognition for electronic records and digital signatures. It was introduced to regulate the information technology sector and was revised in 2008 to address data protection and improving digital security. The Act is organized in thirteen papers with ninety-four sections and four schedules. The term "computer" refers to any electronic, magnetic, optical, or other high-speed data processing system or device that performs logical arithmetic and memory functions through the manipulation of magnetic, electronic, or optical impulses. The Information Technology Amendment Act, 2008 expanded the definition of "communication devices" to include mobile phones, personal digital assistants (PDAs), and other systems that transfer texts, videos, or other media.

The Act covers penalties, compensation, and adjudication. Section 43 states that the person who harms computer systems shall be liable to pay damages by way of compensation to the affected person. Section 43A provides appropriate compensation in cases of failure to protect data at the corporate level of cyberspace administration. Violations are categorized as civil offenses with remedial measures to adjudicate such offences without resorting to police or other investigative agencies. The Information Technology Act of 2000 establishes mandatory jurisdiction for any act or contravention committed outside India by any person, regardless of nationality. This Act covers any act or violation committed outside India by anyone involved in a computer system, computer network, or computers. The regulatory purpose of the government is to pass laws, and the administration and/or judiciary's role is to ensure that these laws are followed and enforced.

The Central Government has made several rules and regulations in accordance with the authority granted by the relevant sections of the Act. These include the Information Technology (Certifying Authorities) Rules, 2000142, which regulate the application and guidelines for Certifying Authorities, the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000143, which specify the procedure for filing applications, the qualifications and experience of adjudicating officers, the terms and conditions of the service of Presiding Officers, the powers of the Cyber Appellate Tribunal, and other standards.

These rules also provide guidelines on information technology security, the process of filing applications, the fees for applications, the process of holding inquiries, the prevention of duplicity, and the steps for compounding contraventions. They also outline the powers of the Cyber Appellate Tribunal and the requirements for the registration of legal practitioners clerks. The Central Government has framed several rules to ensure the security and privacy of information. These include the Information Technology (Security Procedure) Rules, 2004148, which specify procedures for securing electronic records and digital signatures. The Information Technology (Certifying Authorities) Amendment Rules, 2009149, further amend rule 6 of the Information Technology (Certifying Authorities) Rules, 2000.

The rules also outline the appointment of designated officers and nodal officers, their duties, and the procedures for forwarding requests by organizations. They also outline the process of blocking information in emergency cases, the process of court orders for blocking information,

10.48047/jocaaa.2024.33.02.30

expeditious disposal of requests, and the maintenance of records by designated officers. The rules also outline the procedures for interception, monitoring, and decryption of information, as well as the responsibility of intermediaries in handling these matters. They also provide guidelines for monitoring and collecting traffic data or information, ensuring the responsibility of intermediaries, review of directions of competent authority, destruction of records, prohibition of disclosure of intercepted or monitored information, and maintenance of confidentiality. The Cyber Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Chairperson and Members) Rules, 2009153, regulate the terms and conditions of service of the Chairperson and Members, including salaries, allowances, leave, pension, provident fund, travel allowances, leave travel concessions, facilities for medical treatment, oaths of office and secrecy, and declarations of financial or other interest.

In conclusion, the Central Government has framed various rules to ensure the security and privacy of information. The Information Technology Act, 2000 outlines various rules and regulations for the protection of sensitive personal data and information. These include the investigation of complaints, when a Supreme Court Judge can conduct an enquiry, and the provisions of the Departmental Enquires Act, 1972. The rules also outline the power of the judge, suspension of Chairperson or member, subsistence allowance, and the submission of an inquiry report to the President. The Central government has framed guidelines for intermediaries, reasonable security practices, and guidelines for cybercafes. Cyber cafes must only allow users after providing their identity documents and maintain a log register for a minimum period of one year. They should also keep backups of log records and websites accessed using computers at the café. Electronic service delivery rules specify the system of electronic service delivery, steps for notifying the government, creation of a repository of electronically signed electronic records, procedure for making changes in a repository, responsibility of service providers and agents for financial management and accounting, audit of information systems and accounts, and use of special stationery.

The National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties rules specify the location, timing, composition of an Advisory Committee, constituency, functions and responsibilities of CERT-IN, services, stakeholders, policies and procedures, operations of CERT-IN, disclosure of information, seeking information, carrying out functions, and compliance with sub-section (6) of Section 70B of the Act. The Central government has made several rules to regulate the use of digital signatures, security procedures, and certifying authorities in the Information Technology Act, 2000. These rules specify the authentication of information using digital signatures, the creation of digital signatures, verification of digital signatures, and the verification of XML digital signatures. The rules also outline the powers and functions of the Chairperson of the Cyber Appellate Tribunal for efficient disposal of pending matters and implementing statutory provisions for effective functioning.

The rules also cover the preservation and retention of information by intermediaries providing digital locker facilities. These rules specify the appointment of digital locker authority, the location of facilities, the usage of digital locker systems by subscribers, requesters, and issuers, the role of digital locker service providers, the appointment of grievance officers for dispute resolution, suspension and revocation of digital locker accounts, control of digital locker account credentials, fees for opening digital locker accounts, portability of subscriber accounts, annual

10.48047/jocaaa.2024.33.02.30

audits, auditor's relationship with digital locker service providers, confidential information, access to confidential information, and maintenance of reasonable security practices. The 2021 rules define social media intermediaries as entities that primarily or solely enable online interaction between two or more users. Intermediaries with registered users above a notified threshold are classified as significant social media intermediaries (SSMIs), and they are required to observe additional due diligence. The National Cyber Security Policy aims to address the growing ambition of ICT users, including small and large institutions, by providing an integrated vision and strategies for ensuring a secure cyberspace ecosphere. The policy aims to create a National Critical Information Infrastructure protection center and enhance the protection of the infrastructure. It also includes recommendations for collaborative working across all major actors in the public and commercial sectors to secure the nation's information and systems.

India's right to privacy was declared a fundamental right in the 2017 Supreme Court case, leading to the appointment of a data protection committee and the draft Personal Data Protection Bill, 2018. However, the delay in implementing proper data protection law can be costly, as it can lead to identity theft and abuse of personal information.The Information Technology Act, enacted 20 years ago, has been criticized for not addressing the protection of intellectual property and domain-name infringement. Despite these shortcomings, the Act has been enacted to protect internet users and address the increasing number of cybercrimes.

The Budapest Convention, initiated by the Council of Europe in 2001, is a crucial international initiative for developing criminal law. It establishes a common minimum standard of relevant crimes, including nine types of cybercrimes involving human acts and computer networks. By April 2021, 65 states have become members of the Convention, with 12 more signing or having invitations to accesde. The first Additional Protocol to the Convention was added in 2003, focusing on xenophobia and racism committed via computer systems. The 9th Protocol Drafting Plenary was held on 12 April 2021, and stakeholders were invited to participate in an online meeting on 26-27 May 2021. The Second Additional Protocol focuses on enhanced cooperation and disclosure of electronic evidence, ensuring that governments meet their obligations to protect individuals and their rights in cyberspace. The G20 countries expressed an opinion in 2015 that international rule should apply to their cyber activities, and there is a growing consensus that international law should apply to internet activity. States should express their views on how current international law is applied to state activity in cyberspace publicly, and consider the sovereignty of other states, including those outside combat zones.

Conclusion

The Information Technology Act, 2000, was enacted in India in 1999 to regulate the information technology sector, create civil and criminal liabilities for electronic crimes, and ensure legal recognition for electronic records and digital signatures. It covers penalties, compensation, and adjudication for violations, including damages for harming computer systems and appropriate compensation for corporate data protection failures. The Act also establishes mandatory jurisdiction for any act or violation committed outside India by anyone involved in a computer system, network, or computers. The government's regulatory purpose is to pass laws, while the administration and judiciary ensure their enforcement.

10.48047/jocaaa.2024.33.02.30

The Central Government has established various rules and regulations to ensure the security and privacy of information. These include the Information Technology (Certifying Authorities) Rules, 2000142, which regulate the application and guidelines for Certifying Authorities, the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000143, which specify the procedure for filing applications, the qualifications and experience of adjudicating officers, the terms and conditions of the service of Presiding Officers, the powers of the Cyber Appellate Tribunal, and other standards. The Information Technology (Security Procedure) Rules, 2004148, specify procedures for securing electronic records and digital signatures. The Cyber Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Chairperson and Members) Rules, 2009153, regulate the terms and conditions of service of the Chairperson and Members. The Information Technology Act, 2000 outlines rules for the protection of sensitive personal data and information,including investigations, the power of judges, suspension of Chairperson or member, subsistence allowance, and submission of an inquiry report to the President. The Central Government has also framed guidelines for intermediaries, reasonable security practices, and guidelines for cybercafes. The National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties rules specify the location, timing, composition of an Advisory Committee, functions and responsibilities of CERT-IN, services, stakeholders, policies and procedures, operations of CERT-IN, disclosure of information, seeking information, carrying out functions, and compliance with sub-section (6) of Section 70B of the Act. The National Cyber Security Policy aims to secure the cyberspace ecosphere for ICT users, including small and large institutions. It includes recommendations for collaboration across public and commercial sectors to secure information and systems. India's right to privacy was declared a fundamental right in 2017, leading to the appointment of a data protection committee and the draft Personal Data Protection Bill. The Information Technology Act, enacted 20 years ago, has been criticized for not addressing intellectual property protection and domain-name infringement. The Budapest Convention, initiated in 2001, establishes a common minimum standard of relevant crimes, and the G20 countries are considering applying international law to internet activity.

References

1. T. Bolling and R. G. Lennon, "Viewing DevOps Security Processes through An Applied Cyberpsychology Lens," *2023 Cyber Research Conference - Ireland (Cyber-RCI)*, Letterkenny, Ireland, 2023, pp. 1-6, doi: 10.1109/Cyber-RCI59474.2023.10671453.
2. Parkin, S., Krol, K., Becker, I., & Sasse, M. A. (2016). Applying cognitive control modes to identify security fatigue hotspots. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).
3. Kam, Hwee-Joo and D'Arcy, John, "A DEVOPS PERSPECTIVE: THE IMPACT OF ROLE TRANSITIONS ON SOFTWARE SECURITY CONTINUITY " (2023). *ECIS 2023 Research-in-Progress Papers* . 86.
4. Salminen, H. (2023, June). We see what we want to see: Pitfalls of Perception and Decision-making in Security Management. In European Conference on Cyber Warfare and Security (Vol. 22, No. 1, pp. 669–677.
5. Garcia, S. Jones, and R. Patel, "Collaborative Approaches to Cybersecurity: A Cross-Disciplinary Perspective," *ACM Transactions on Computing Security* , vol. 24, pp. 1–23, 2021.
6. Johnson and B. Smith, "Understanding Human Behavior in the Digital Realm," *Journal of Cyberpsychology and Computer Science* , vol. 8, pp. 45–56, 2020.

10.48047/jocaaa.2024.33.02.30

7. Smith and R. Thomas, “Fostering a Culture of Security in DevOps Teams: Strategies and Best Practices,” *Journal of Cybersecurity Education and Training* , vol. 13, pp. 89–102, 2019.
8. Lee and G. Wang, “Anchoring Bias in DevOps Security: Implications for Risk Assessment,” *Journal of Cybersecurity Studies* , vol. 8, pp. 67–80, 2018.
9. Lee and Y. Wang, “Influence of Behavioral Nudges and Incentives on DevOps Security Behavior,” *Journal of Cybersecurity and Privacy* , vol. 8, pp. 95–110, 2018.
10. J. Gupta, et al., “Time Pressure Compromising Security in DevOps Environments: A Case Study,” *Journal of Cyberpsychology and Computer Science* , vol. 7, pp. 145–158, 2019.
11. X. Xiong, Q. Yao and Q. Ren, "Mission-Oriented Security Framework: An Approach to Embrace Cyber Resilience in Design and Action," *2023 7th International Conference on Cryptography, Security and Privacy (CSP)*, Tianjin, China, 2023, pp. 54-58, doi: 10.1109/CSP58884.2023.00016.
12. Kott, A., Linkov I., eds. (2019). *Cyber Resilience of Systems and Networks*. Switzerland : Springer. https://doi.org/10.1007/978-3-319-77492-3.
13. Y. Huang, L. Huang, and Q. Zhu, “Reinforcement learning for feedback-enabled cyber resilience,” *Annu. Rev. Control.*, vol. 53, pp. 273–295, 2022. [Online]. Available: https://doi.org/10.1016/j.arcontrol.2022.01.001
14. D. Liu, Y. Liu, Z. Liu, X. Zhang and X. Zhang, "Analysis and Reflection on the Situation of Industrial Information Security Ransomware Attacks," *2023 8th International Conference on Data Science in Cyberspace (DSC)*, Hefei, China, 2023, pp. 354-358, doi: 10.1109/DSC59305.2023.00057.
15. L. Xie and J. Wu. “Research on Challenges and Defense Countermeasures of Industrial Internet Information Security,” *Information and Computer (Theoretical Edition)*, 2023, 35 (07): 228–230.
16. X. Wang, “Recent global cyber security situation and trend analysis,” *Communications Management and Technology*, 2022, no. 03, pp. 53–55.
17. G. Liu and W. Lyu, “Overview of Active Hacker Groups around the World in 2021,” *Information Security and Communications Privacy*, 2022, no. 01, pp. 17–31.
18. E. S. Basan, V. D. Mikhailova and M. V. Martynenko, "Security Assessment of Technological Process for Smart Manufacturing," *2023 International Russian Automation Conference (RusAutoCon)*, Sochi, Russian Federation, 2023, pp. 1010-1015, doi: 10.1109/RusAutoCon58002.2023.10272843.
19. A. Basan, E. Basan, and A. Gritsyni, “Overview of information security issues for a robotic system,” *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, Xi'an, China, 2019, pp. 1275–1279, doi: 10.1109/ICCT46805.2019.8947054.
20. G. Ravikumar, B. Hyder, and M. Govindarasu, “Next-generation CPS testbed-based grid exercise - synthetic grid, Attack, and Defense Modeling,” 2020 Resilience Week (RWS), Salt Lake City, UT, USA, 2020, pp. 92–98, doi: 10.1109/RWS50334.2020.9241284.