JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

THE BATTLE AGAINST CYBER SECURITY THREATS AND HURDLES

[1]Mrs.P.ANANTHI, [2]Mr.M.VIGNESH, [3]Mr.D.VENGATESAN
[1]Assistant Professor, [2]PG Student II-M.Sc Computer Science, [3] PG Student II-M.Sc Computer Science

PG & RESEARCH DEPARTMENT OF COMPUTER SCIENCE,
E. G.S. PILLAY ARTS & SCIENCE COLLEGE-NAGAPATTINAM-611 002, TAMIL NADU, INDIA.

Abstract: The Internet has grown important to modern life, providing services like e-commerce, online education, and gaming, but it has also led to a growth in cybercrime. In India, cybercrime complaints reached an average of 7,000 daily in early 2024, a considerable rise from prior years, with over $120 crores lost to cyber fraud. Globally, roughly 600 million cyberattacks occur daily. Cybercriminals deploy strategies such as hacking, credential theft, and data manipulation to access and modify sensitive information. Factors including outdated software, security breaches, and online hacking tools contribute to the rise of these crimes. As technology evolves, particularly in the hands of younger generations, the threat of cyberattacks is certain to grow. Securing cyberspace remains a complex and challenging endeavour, as it consists of huge networks, much like the human brain's neural connections.

Index Terms**:** Internet, cybercrime, e-commerce, online education, gaming, cyber-attacks, India, cyber fraud, hacking, credential theft, data tampering, security flaws, obsolete software, cyber security, technology, younger generations, securing cyberspace, networks, neural connections.

Introduction

Currently, technology is fully dependent on the Internet. In the ultramodern world, people may now readily reach anything over the internet. Everything is possible with the help of the internet, comparable to e-commerce, online shopping, online bargains, online schooling, gaming, etc. The cybercriminal attacks or changes the data via the internet. The Indian Cybercrime Coordination Center (I4C) recorded a normal of 7,000 cybercrime complaints per day in the first four months of 2024. This is 113.7 further than 2021–2023 and also 60.9 advanced than 2022–2023. In September 2024, the loftiest number of instances was registered on the cybercrime gate. So several people have lost over $ 120 crore to cyber crime in 2024.

According to Microsoft’s digital protection study, there are over 600 million cyberattacks every day around the world. Security is the process of guarding the electronic information from unauthorized persons. Then some cybercriminals use attack strategies similar to hacking, credential stealing, data manipulation, regard kidnapping, etc. These sorts of cyber attacks are substantially geared at penetrating, destroying, or changing sensitive information by using the internet.

The key factors behind the increase in cybercrime include the usage of inappropriate software, expired security tools, programming defects, internet hacking tools, etc. In the current generation, the five-year-old child utilizes mobile. Perhaps in the future, the internet operation will be increased as the same as different sorts of attacks may also increase in the following periods. The mission of preserving cyberspace is the most intricate and hard process. Cyberspace is a virtual domain, and it is used to connect different computer systems. For example, the human brain has millions of neurons, as cyberspace has innumerable connections and networks.

Cyber security

According to the IT Act, Cybersecurity means the protection of information, computer systems, communication devices, and networks from unauthorized persons by using the internet. Cybersecurity is very important for every individual, business, government, and organization to protect digitized data. It is a shared responsibility between people, organizations, and the government for a secure digital environment. Three things are used to create defensive cyber security, such as people, processes, and technology. Users must understand the basic principles of security by using strong passwords and avoiding spam messages, being aware while using social media. All organizations must have a framework for dealing with data from cyberattacks. The basic common technology used to protect these entities includes firewalls, Domain Name System, Malware protection, and antivirus software.

What Makes Cyber Security Crucial?

Cyber security is very important because it protects data from cyberattacks and cybercrime that can damage businesses, communities, and lives. Here are some reasons why cybersecurity is important. Organizations must maintain security standards to protect customer data and non-compliance can lead to penalties. Digital systems like energy, communication, and transport are important to security, so organizations need a cybersecurity approach. Cyberattacks can target critical infrastructure, government systems, and military installations. Cybersecurity requires preventing, spotting, and fighting many connected-to-the-internet dangers, including the aforementioned hack attempts, malware contaminations, data breaches, and different cybercrimes.

Managing Cyber Security Threats

All the attack's pitfalls are determined by three factors challenges (who is attacking), excrescencies (how they're attacking), and consequences (what the attack does). Benefit assessment for information structure is regarded as critical to successful data defense.

Branches of Cyber security

There are many types of cybersecurity methods to protect digital systems from malicious and accidental threats. It is so helpful to understand the six most commonly referenced types of cybersecurity. Cybersecurity can mean different things depending on which aspect of technology you are managing various types of cybersecurity enable organizations to define their various systems.

Network security

Network security includes software and hardware solutions that protect against incidents that result in unauthorized access or service disruption. The main aim of network security to protect the computer network from unauthorized access. Network technologies such as Firewalls, Intrusion detection systems (IDS), Virtual private networks (VPM), and Network segmentation. The majority of cyber-attacks start over a network and also network cyber security is designed to monitor, detect, and respond to network threats. Sometimes we use free wi-fi in public areas Third-party starts tracking your phone over the internet, so avoid using free networks because free networks do not support security.

Application security

Application security is protecting the application from intruders. This application security is used to resolve bugs in code and implement cybersecurity measures to protect against third-party persons. Most vulnerabilities are introduced during the development and publishing stages. Application security is used to help identify flaws during the design and development phases and also helps to protect against these vulnerabilities. A subset of application security is web application security.

Information Security (InfoSec)

Information security focuses on the protection of data—whether digital or physical—from unauthorized access, disclosure, modification, or destruction. It ensures that information is kept confidential, integral, and available when needed.

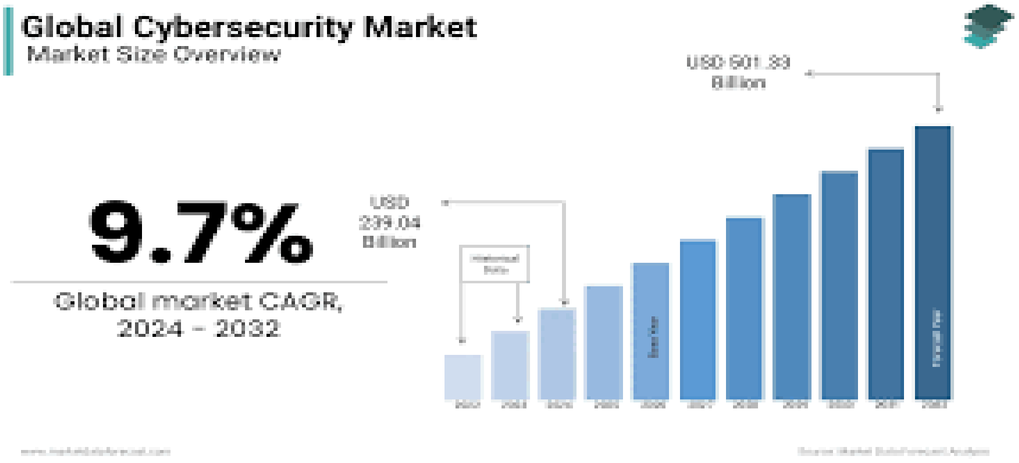
Key Components:

Confidentiality: Ensuring that information is only accessible to authorized individuals.

Integrity: Ensuring that data is accurate and hasn't been altered in an unauthorized way.

Availability: Ensuring that data is available and accessible when needed by authorized users.

Scope: InfoSec can encompass not just digital data but also physical documents, intellectual property, and more.



Cloud Security

Cloud security refers to the practices, policies, and technologies designed to protect data, applications, and services hosted in cloud environments. It includes measures to safeguard against unauthorized access, data breaches, data loss, and attacks such as malware or denial of service. Cloud security ensures that sensitive information is kept safe while maintaining the availability, integrity, and confidentiality of cloud-based resources. It involves both the cloud service provider's security infrastructure and the user's responsibilities for securing their own data and applications within the cloud.

Cloud security challenges include:

1. **Insider threats:** Authorized users, like employees, contractors, or partners, may abuse their privileges to harm the business.
2. **Insecure interfaces and APIs:** Attackers can use insecure interfaces and APIs to bypass security controls, access sensitive data, or disrupt the cloud infrastructure.
3. **Misconfiguration:** Cloud resources may be set up with weak security controls or improper access permissions.

IoT Security

Internet of Things (IoT) security is a branch of cybersecurity that protects connected devices from threats. IoT devices are physical devices that can connect to a network wirelessly. The ability to access these devices through a smartphone or through a computer is called IoT. These devices are accessed from a distance.

For example, an Air conditioner sensor can gather the data regarding the outside temperatures, and accordingly adjust its temperature to increase or decrease it with respect to the climate. Similarly, refrigerators can also adjust their temperature accordingly

Mobile Security

Mobile security is a cybersecurity strategy that protects mobile devices from cyber threats. It includes protecting data on the device, as well as the network and endpoints connected to the device.

What are the threats to mobile security?

1. **Malicious applications and websites:** These can steal credentials, compromised accounts, and cause data loss
2. **Data leaks:** These can expose private information
3. **Spyware:** This can monitor a user's activity
4. **Social engineering attacks:** These can trick users into sharing sensitive information
5. **Broken cryptography:** This can happen when app developers use weak encryption algorithms

How can you safeguard your mobile device against cyber-attacks?

1. Use a strong passcode or biometric lock.
2. Use two-factor authentications.
3. Install antivirus software.
4. Keep your device updated.
5. Download apps from trusted sources.
6. Review app permissions.
7. Use a VPN on public Wi-Fi.

Essential Elements of Cybersecurity

1. **Confidentiality:** Keeping sensitive data and information private by limiting access to just those who are authorized.
2. **Integrity:** Upholding the reliability, correctness, and consistency of data and systems.
3. **Availability:** System and data availability refers to making sure they are available and useful when required.
4. **Authentication:** Authorization is verifying users' and devices' identities during authentication, which helps prevent unauthorized access.
5. **Authorization:** The authorized person is the only one who can access the data, which is known as authorization.
6. **Nonrepudiation:** The provision of proof demonstrating the provenance and reliability of digital transactions.
7. **Trust Maintaining and Confidence:** Creating and maintaining confidence in online interactions, digital transactions, and other kinds of online services is made possible by cyber security. Cyber security helps people, businesses, and society at large feel more secure by safeguarding user data, privacy, and the security of online platforms.

Types of digital security threads

Online security threats include malware, phishing, and DDoS attacks.

Malware

1. A type of software that can damage, disrupt, or gain unauthorized access to a computer system.
2. Includes viruses, worms, trojans, spyware, and ransomware.
3. Can infiltrate a system through a link in an email or on an untrusted website.
4. Can collect sensitive data, destroy data, or shut down a system.

Phishing

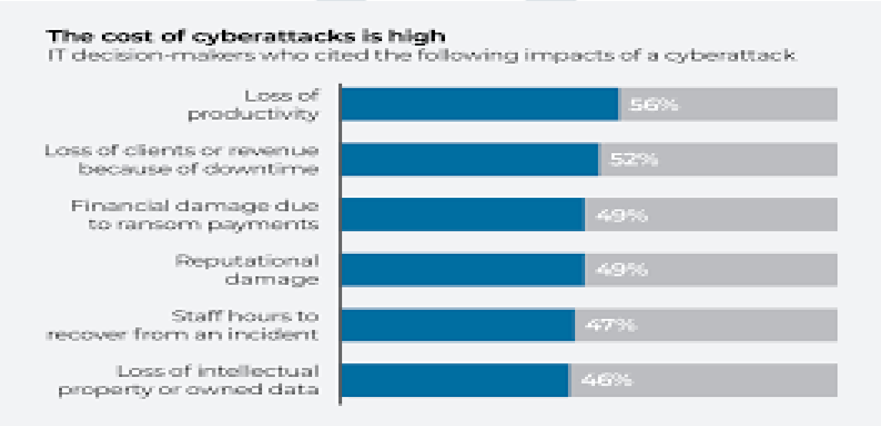
1. A cyber-attack where criminals impersonate a legitimate source to request sensitive information
2. Commonly targets victims via email
3. Can request passwords, bank account details, or other sensitive information

DDoS attacks

1. A cyber-attack that attempts to disrupt a network by overwhelming it with traffic.
2. This can be done by sending a large amount of data or illegitimate requests.
3. Can target a website, server, or other network resource.

Government's Responsibility in Cybersecurity

The government's role includes not only the definition of government infrastructure but also assistance in the protection of networks that are not owned by the government. Every single government agency is now responsible for the data security of their own networks, and many of them have sector-specific duties for CI in accordance with the existing regulations. the legislation. The National Cyber Security Policy is a legislative framework that was formed by the Department of Electronics and Information Technology (Deity), which is part of the Ministry of Communication and Information Technology in the Indian government. Its purpose is to protect both public and private networks from being attacked by cybercriminals.



Personal information (of web users), information pertaining to financial and banking transactions, and data pertaining to sovereign entities are all intended to be protected in accordance with the regulation. It was especially essential in light of recent leaks from the National Security Agency (NSA) that indicated that government agencies in the United States are spying on Indian consumers, who have neither legal nor technological defenses against this act. Cyberspace, according to India's Ministry of Communications and Information Technologies, is a varied ecosystem comprised of human activities, software applications, and the worldwide dissemination of information and communication technologies.

According to several publications and research, India's National Cyber Security Policy of 2013 includes a number of flaws and shortcomings. Despite the announcement of the strategy, India is not yet prepared to deal with cyber threats. In addition, the proposal was not adopted until November 2014. (until 21 November 2014). India's data security concerns are only going to become worse, thus decisive action is necessary. India's proposed projects, such as the National Cyber Coordination Centre and the National Critical Information Infrastructure Protection Centre (NCIIPC), could enhance the country's cyber security and critical infrastructure protection. Now it shall observe how Cyber Security Strategy 2020 safeguards cyberspace.

Benefits of cyber security

1. **Safeguarding Information**: It ensures that personal, financial, and business data remains secure from unauthorized access, reducing the likelihood of data breaches.
2. **Threat Mitigation**: With cybersecurity, organizations can effectively identify and block potential cyber threats, like viruses, ransomware, and phishing, before they cause harm.
3. **Operational Security**: It helps maintain the normal functioning of systems and networks, preventing disruptions that could lead to lost productivity or system downtime.
4. **Trustworthiness**: By protecting data, cybersecurity builds customer trust, showing that their sensitive information is handled securely and responsibly.
5. **Compliance Assurance**: Many industries are governed by strict data protection laws. Cybersecurity helps businesses meet these legal requirements, avoiding fines and reputational damage.
6. **Preserving Brand Image**: By preventing cyber incidents, organizations protect their reputation and avoid the negative fallout that can come from a data breach or security lapse.
7. **Protecting Business Assets**: Cybersecurity ensures that critical business information, intellectual property, and proprietary systems remain shielded from theft or misuse.
8. **Cost Efficiency**: Though implementing cybersecurity involves costs, it ultimately saves money by preventing expensive data breaches, recovery efforts, and legal consequences

Challenges of Cyber Security

1. **Protection Against Cyber Threats**: Cyber security plays a crucial role in defending systems from potential risks such as hacking, malware, ransomware, and phishing. Without it, organizations could face serious consequences like data theft, financial losses, and system damage.
2. **Maintaining Data Accuracy**: Effective cyber security practices ensure that data remains intact and unaltered by unauthorized parties, helping organizations preserve the integrity of their information.
3. **Guarding Personal Information**: For individuals, proper cyber security measures protect sensitive data like financial details, passwords, and private messages from theft or misuse.
4. **Ensuring Business Continuity**: A robust cyber security framework allows businesses to keep operations running smoothly, even when under attack. It minimizes the likelihood of downtime, ensuring that key systems remain functional.
5. **Building Customer Confidence**: Businesses that prioritize protecting customer data earn trust. This enhanced confidence can strengthen customer relationships and encourage loyalty.
6. **Meeting Regulatory Standards**: Compliance with industry-specific cybersecurity regulations, such as GDPR and HIPAA, helps organizations avoid fines and enhances their credibility by adhering to legal requirements.
7. **Minimizing Financial Impact**: By preventing data breaches and cyber attacks, cyber security reduces the risk of costly consequences, such as penalties, legal fees, and lost revenue.
8. **Boosting Productivity**: Strong security protocols help avoid disruptions, allowing employees to perform their tasks without delays or interruptions caused by security breaches.

Conclusion

As the world becomes more reliant on the internet for everyday tasks, the threat of cybercrime continues to grow, posing serious risks to both security and privacy. The sharp rise in cyberattacks, especially in nations like India, underscores the immediate need for stronger cybersecurity frameworks. Outdated security systems and vulnerable online platforms play a significant role in this growing problem. With technology advancing rapidly and younger generations becoming more digitally engaged, the challenge of securing cyberspace is only set to increase. To safeguard sensitive data and preserve trust in digital environments, prioritizing cybersecurity is essential. Strengthened security protocols, greater awareness, and ongoing innovation will be crucial in addressing the dangers posed by cybercriminals.

Reference

[1].Mr.M.Jayakandan and Dr.A.Chandrabose,"Land Weber Iterative Supervised Classification and Quantized Spiking Network for Crime Detection Emotion Analysis", International Journal of Intelligent Systems and Applications in Engineering, Volume 12, No 21S, (**2024**), Page No: 2219-2224, ISSN NO: 2147-6799 (**G-II-SCOPUS**).

[2]. Mrs.P.Ananthi and Dr.A.Chandrabose, "The Socio-technical Opportunities and Threats of Crowdsensing", The Scientific Temper, Volume: 15 (spl-1), 2024, Page No.:291-297, ISSN Print: 0976-8653 and E-ISSN: 2231-6396 (**G-II_WEB OF SCIENCE**).

[3]. Mr.M.Jayakandan and Dr.A.Chandrabose, "Emotion Analysis Using Iterative Supervised Classification Algorithm for Crime Detection", International Journal of Intelligent Systems and Applications in Engineering, Volume: 12, No 21S, (**2024**), Page No: 2225-2231, ISSN NO: 2147-6799 (**G-II-SCOPUS**).

[4]. Mrs.P.Ananthi and Dr.A.Chandrabose, "Exploring Learning-Assisted Optimization for Mobile Crowd Sensing", The Scientific Temper, Volume 15 (spl-1), 2024, Page No: 283-290. ISSN Print: 0976-8653 and E-ISSN: 2231-6396 (**G-II_WEB OF SCIENCE**).

[5]. Mr.M.Jayakandan and Dr.A.Chandrabose, "An ensemble-based approach for sentiment analysis of covid-19 Twitter data using machine learning and deep learning techniques", The Scientific Temper Volume: 15 (spl-1), **2024**, Page No:114-120, ISSN Print: 0976-8653 and E-ISSN: 2231-6396 (**G-II_WEB OF SCIENCE**).

[6]. Mrs.P.Ananthi and Dr.A.Chandrabose, "Volterra Integral Equation and Logistic Drop-Offloading for Collaborative Mobile Fog Crowd Sensing", International Journal of Intelligent Systems and Applications in Engineering, Volume: 12, No 21S, (2024), Page No: 2186-2192, ISSN NO: 2147-6799 (**G-II-SCOPUS**).

[7].Mr.M.Jayakandan and Dr.A.Chandrabose, "Machine Learning Classifications for Automatic Sentiment Analysis on Twitter", Indian Journal of Natural Sciences Volume:15, Issue: 86, **October-2024**, Page No: 81858-81867, ISSN: 0976 – 0997 (**G-II_WEB OF SCIENCE**).

[8]. Mrs.P.Ananthi and Dr.A.Chandrabose, "Utilizing Mathematical Modelling and Offloading to Conduct Crowdsensing in A Collaborative Setting", International Journal of Intelligent Systems and Applications in Engineering, Volume: 12, No 21S, (2024), Page no: 2193-2197, ISSN NO: 2147-6799 (**G-II-SCOPUS**).