GNA Journal of
Management & Technology
Vol. XV, No. I, June 2024

PERSPECTIVES OF VARIOUS CYBER SECURITY THREATS AND DEFENSE MECHANISMS IN THE MODERN WORLD

Dr. Sumit Chopra*[1] , Isha Kareer[2], Er. Gagandeep Singh[3], Rajesh Sharma[4]

[1]*Associate Professor GNA University, Phagwara, India,*
[2]*Student GNA University, Phagwara India*
[3]*Assistant Professor GNA University, Phagwara*
[4]*Associate Professor GNA University ,Phagwara India*[4]

Email:- sumit.chopra@gnauniversity.edu.in

Abstract

The focus on cyber security has increased, requiring the involvement of researchers, educators, and companies to securely safeguard information systems. With the growing need for digital transformation, individuals and organizations encounter constantly evolving cyber risks. The increasing prevalence of cybercrime has made the security of digital assets crucial. Digital documents and important files are open to hacking without proper security measures in place, which puts governments, businesses, financial institutions, and military groups at serious risk. This article provide the state of art for cyber security, challenges, tactics and global trends of the cyber security. To stay ahead of the curve in cyber security, a systematic review is conducted to uncover the latest trends, challenges and state of art in cyber security. In addition, we discuss the future path of cybersecurity, outlining potential tactics and methods for dealing with the growing cybersecurity threats, the developing patterns, and advancements such as Artificial Intelligence (AI) and machine learning (ML) for identifying and automating responses to cyber threats. This study emphasizes the cutting-edge methods and strategies in cyber security that are crucial for safeguarding private data. It provides a thorough overview of the changing cyber security scene by diving into the present issues, looking at different kinds of cybercrimes, and examining their significant effects.

Keywords:Cyber security, CIA triads, Cybercrimes, Tools for detection, Cybercrime defense methods.

Introduction

Today, the fastest growing frame in everyday life is the Internet. Various technologies are changing, such as online transactions, e-commerce, e-government, and more. In today's environment, more than 65% of transactions are done online, which requires high transaction security. In today's era, every feature of our survival depends on the computer and on various electronic devices. The main point is that the opportunity in cyber security is not bound to the security of the IT industry; in other areas, such as cyberspace, cloud computing is also requiring high security. Therefore, the initial step in protecting information and preventing anyone from accessing it is a security program. There are a variety of security programs used by various people and countless organizations to protect their software from

hackers. Today's world heavily relies on electronic technology, and the difficult problem is defending this electronic data from cyberattack (Smith et al., (2020), Li et al., (2021). The main aim of cyberattacks is to cause financial damage to businesses. These harms include PC viruses, data delivery services (DDS), knowledge destruction, and other attack vectors. For this purpose, different organizations use different solutions to prevent data damage from cyberattacks. Intellectual property, financial information and data, and any personal data that can be sensitive information for unauthorized access could have a negative effect. This also causes reputational damage. Therefore, a cybersecurity scheme is important to protect important and sensitive information. Encryption is the most powerful and crucial tool for protecting sensitive data (Li et al., (2021). The analysis of a cyberattack is summarized in Fig. 1

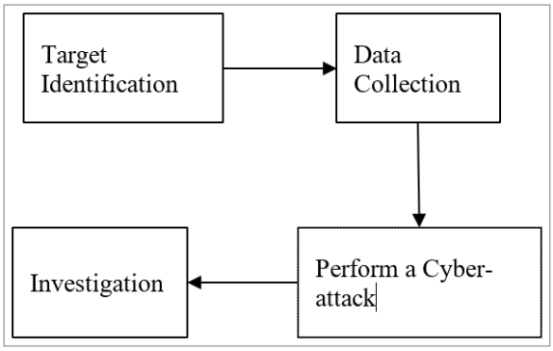


Fig. 1. Analysis of a cyberattack [2]

Cybersecurity is the protection of servers, electronic gadgets, mobile devices, networks, computers, and sensitive data information from malicious attacks. Cybersecurity is used for the protection of internet connected systems, including hardware, software, and data, against cyber threats. Security is also important for the protection of systems, applications, networks, and information (Roldán-Molina et al., 2017).Cyber security makes sure that only authorized users have access to that information for added protection.

Recent studies highlight the severity of these threats and the necessity for advanced security measures. In (Admass et al., 2024), emphasis is made on cyber-attacks and the critical need for continuous improvement in defense mechanisms. In [Prakash et al. , 2022], innovative encryption techniques as pivotal tools for protecting sensitive data were discussed. These studies, among others, underscore that intellectual property, financial information, and personal data are all vulnerable to unauthorized access, which can result in significant reputational damage.

In (De Azambuja et al. , 2024) and (Jada et al. , 2023), the various cyber threats to the organizations were discussed and how AI can yield benefits like threat intelligence, automation and improved cyber

defence. In addition to it, authors also highlighted the various challenges like need of high quality data and adversarial attacks which throw light on the inefficiency of AI in cyber security. In (Botta et al. , 2023) the cyber security of Robots were analysed from the aspects of Operating system and Physical and Network security. It was concluded, that Robots software, data, hardware and software are the most venerable parts and needs to be protected.

Processes and policies give a framework for governance and help in defining practices that are measurable gradually. Processes inform responsive IT controls and initiative-taking. This means that there are various processes in place to support the integrity of our security system. Examples are physical barriers, such as safe spaces, which make hardware accessible and secure. Intelligence controls, such as regular audits and reviews, ensure that software and data are managed securely according to best practices. It clarifies how you can collect, process, store, protect the organization, reply to threats, and give information. Technologies are the software and hardware that sectors use to attain credible cyber security. These are mechanisms by which IT personnel establish processes to prevent breaches of their IT infrastructure. May include behavioral analytics to monitor user and employee behavior and transactions. This could be a breach detection system that notifies malware or hackers or a vitrified response system that verifies the victims' credentials.

Various technologies can be combined to make more hardened systems that make it harder for cyber threats to penetrate personal data. Software, networks, and hardware that support people and business processes. Three main objects essential to threats are routers, managed devices, and endpoint strategies like PC's. A security system is used to protect modern technology from cybercrime. The main aim of the security system is to filter the data packets and choke the unauthorized packets. Except for the security system, we used various technologies to defend the data from data breaches, like malware defense, antivirus tools, email security results, DNS pass-through filters, and the rest (Sheth et al. , 2021). A cybersecurity strategy is more than just defending against cyber threats.

The three main objectives of cybersecurity are to ensure the protection of data. The cyber security communities provide a triangle of three related principles: Confidentiality, Integrity, and Availability to defend the information from cybercrimes. This principle is known as the CIA triad and is shown in Fig. 2

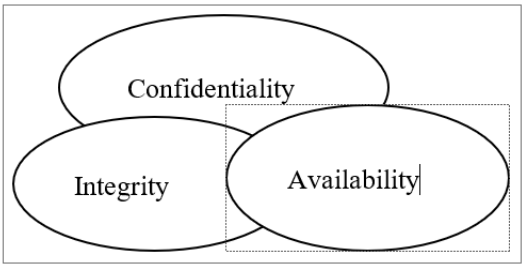


Fig. 2. CIA Triad

This first principle is to prevent unauthorized access or disclosure of company information while ensuring that only authorized people have access. Confidentiality is said to be compromised when an organization's data is accessed, damaged, compromised, or deleted by someone without proper authorization. This means that the data must not be threatened or accidentally (unnecessarily or maliciously) changed by someone without proper authorization. This CIA principle verifies that data is protected from unauthorized changes, both real and accurate. When changes occur, extraordinary measures must be taken to defend sensitive information from loss and to recover lost data quickly from such events. Availability means that authorized users can easily access information whenever they need it, minimizing disruptions and failures. Keep information accessible and useful to unauthorized persons (Roldán-Molina et al. , 2017). IT information must be continuously and easily accessible to authorized persons.

This paper is organized into different sections to highlight the various perspectives of cyber security in modern world. Section 2 explains the different classifications of cybercrimes followed by explanation of categories of Cyber security in Section 3. Section 4 explains the common cyber security threats followed by tools for detecting cybercrime in Section 5 . The defence methods of cyber crimes are discussed in Section 6 and followed by various case studies explained in Section 7. Finally , the finding are concluded in the Conclusion section.

CYBER CRIME

Crimes committed by using a network or computer or any illegal activity like committing fraud, stealing identities, trafficking child pornography, intellectual property, and so forth. that uses a computer is known as cybercrime. Computer crimes are considered illegal, unethical, or unauthorized behavior by people relating to the automatic processing and transmission of data used on computer systems and networks. Cybercrimes or electronic crimes are any act that intentionally harms the victim's reputation, causes physical or mental harm, or directly or indirectly causes the loss of money or information using the Internet or electronic devices. The criminal motive behind most cybercrimes is to attack the information of individuals, businesses, or governments. Attacks do not occur in the physical body but in the computer-generated bodies of individuals or companies, which are a collection of informational attributes that define individuals and organizations on the internet. In the digital world, our computer generated identity is an essential part of our everyday lives. Also, critical infrastructure may be at risk and affect water resources, medical services, energy distribution, national communications, loss of online business and consumer confidence, financial services, and shipping. In the digital economy, loss of personal financial resources, business assets, and later emotional trauma, costs of commercial companies and government agencies to rebuild their credit histories, identities, and companies; account costs to improve cyber security measures; and costs of

law enforcement time and resources (Frunza, ,2016) , (DeTardo-Bora et al. , 2016).

The four main classifications of cybercrimes are:

Cybercrimes against individuals: In the email spoofing, the headers of emails are counterfeited so that the email appears to come from one reputed source when it comes from another source that is from Confidentiality Integrity Availability hackers. Spamming refers to sending multiple copies of mass emails, such as junk mail or chain letters.

When defamation is committed using a computer or the Internet, this type of cybercrime is referred to as Cyber-defamation. Cyberstalking refers to tracking a person's activities online. This type of cybercrime happens with the help of already existing protocols such as email, chat rooms, user network groups, and so forth (Team et al. , 2022).

Cybercrimes against Organizations: Unauthorized computer access: access to a computer or network without the owner's permission. a) Modification or deletion of data: Unauthorized modification of data. b) Computer eavesdropping: Criminals read or copy personal information but do not remove or change the data. Denial of Service constantly floods Internet servers with fake requests that prevent legitimate users from using the host or cause the server to crash. A virus is a self-executable program; it is a kind of computer program that infects other computers by changing them to include versions of them. Worms do not need a host to attach themselves. Email bombing is sending mass emails to an individual, company, or email server that eventually cause it to fail. When a ridiculously small amount is stolen and added to a larger amount, Salami attacks were used to commit financial crimes. Logic Bomb is an event-dependent program. Computers may fail, viruses may release, or other harmful things may occur as soon as the specified event occurs. Diddling of data is a type of attack in which the raw data is changed before it is prepared by the computer and is changed again after the processing of the data is complete.

Cybercrimes against Property: Credit Card Fraud is a fraud committed using a credit card. This usually happens when someone learns your card number or your card is stolen. Intellectual property crime is a type of crime that includes software theft. Copyright infringement is the use of copyrighted material without proper permission. Trademark infringement is the use of a trademark and related rights without the permission of the true owner. Theft of source code from the computer is the theft, destruction, or misuse of computer source code. Theft of internet time happens when the internet time is used by an illegal person and actually paid for by someone else (Colorossi , 2015).

Cybercrimes against Society: Mark sheets, currency notes, fake certificates, and so forth. can be forged (false) using computers. In cyberterrorism attacks, computer resources can be used to harass people and perform terrorism activities. Web jacking is a type of cybercrime in which attackers gain access and get full control over the website for money (John, 2016).

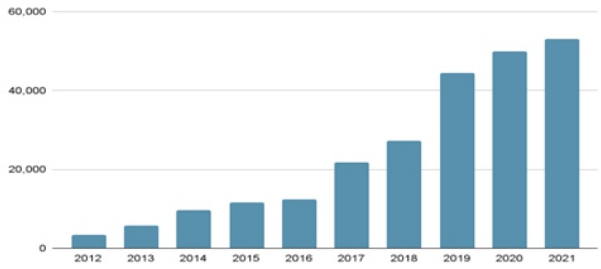
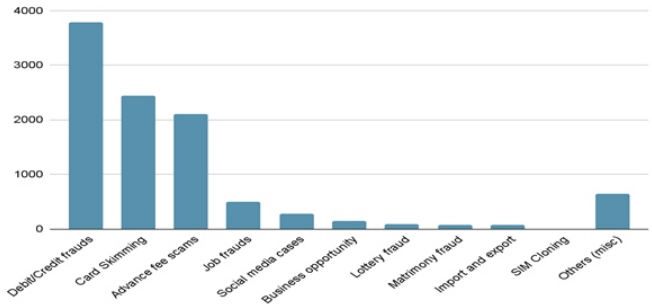


Fig. 3. Number of cybercrimes across India (*Statista of cybercrimes across India from 2012 to 2021)[36]*

The number of cybercrimes that took place in India from 2012 to 2021 has been plotted in Fig. 3. We can see a upside trend in the number of cybercrimes being reported and the number of cases are rising with each passing day.

The various types of cybercrime that took place in India has been summarized in Fig. 4. From all types of crime, Debit/Credit fraud tops the chart followed by card skimming and advance free scams. Jobs frauds and social media cases are also notable in the list. Some of other types of frauds which are taking place is when one lures other person for business opportunity and does fraud with him. Lottery frauds are also taking place in notable numbers in India along with memory and import-export fraud. One of the new types of fraud that is taking place is SIM cloning and the attacker is able to get the OPT's required for doing illegal transactions on other person behalf.



CATEGORIES OF CYBER SECURITY

Various cyber-attacks occur on networks and its security solution is designed to block and detect attacks, which is summarized in Fig. 5. Various solutions include data and management, including special-purpose Data Loss Protection, Identity Access Management, Network Access Control, and Next Generation Firewall controls. It is far secure from the net. In the developed era, the network threat prevention era contained NGAV (Next Generation Antivirus), Sandboxing, IPS (Intrusion Prevention System), and CDR (Content Disarmament and Reconstruction). Additionally essential are threat searching, network analytics, and automatic security orchestration and response (SOAR) technologies.

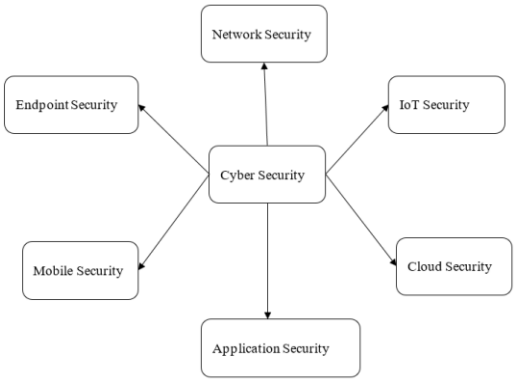
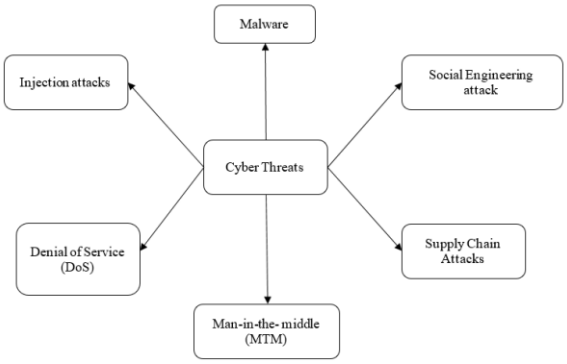


Fig. 5. Categories of cyber security



Internet of Things (IoT) devices without a doubt boom productivity; however in addition, they expose corporations to new cyber threats. IoT safety protects related gadgets by discovering and classifying them, automatically segmenting them to manipulate network activity, and using IPS as a digital blotch to save utilization in opposition to unsafe IoT gadgets. In a few cases, tool firmware may be hardened by small elements to prevent utilization and runtime attacks. The Zero Trust Security Model prescribes the creation of shards, irrespective of where the information resides. One way to try this with mobile workers is to use endpoint security. Endpoint security enables companies to secure user devices, which include desktop computers and laptops, with information and web security control, ATP includes anti-phishing attacks, anti-ransomware attacks, and endpoint detection and response (EDR). You may use technology that offers a forensics solution. As groups increasingly include securing the cloud, it has become a concern. A cloud security schedule includes guidelines, services, cybersecurity solutions, and controls that assist in protecting an employer's whole cloud deployment (applications, data, infrastructure, programs, facts, and so forth.) from attacks. Many cloud providers provide security solutions; however, they may be regularly inadequate to attain enterprise-level security inside the cloud. Cloud environments require third-party solutions to prevent data breaches and attack plans. Protecting information in the cloud (software-based) and monitoring and removing

the risk of on-site attacks (Vaddi et al. , 2020) and (Ficco et al., 2017). Web applications, like other Internet applications, are targeted with the aid of attackers. Since 2007, OWASP has tracked the top ten threats to important web application security, which include SQL injection, misconfiguration, cross-site scripting, and broken authentication. Application security can prevent OWASP‹s top ten attacks. The usage of hardware and software programs (antivirus programs, antivirus packages, encryption, firewalls, and so forth.) protects the device from external threats that can hinder the development of applications. Mobile security prevents those attacks that protect our operating system and devices from root and jailbreak.

COMMON CYBER SECURITY THREATS

There are various cyber security related threats like malware, social engineering attacks, injection attacks, phishing attacks, man-in-the-middle attacks and supply chain threats, which are summarized in Fig. 6

Malware*:* Malware is defined as malicious software, together with phishing, worms, Trojan horses, viruses, and malware, which provide illegal access to damage a computer. Malware attacks are increasing, and it is designed to inspect common detection tools, along with antivirus equipment that searches for malicious attached documents. Most malware is self-replicating, meaning that when infecting a particular system, it enters the Internet, after which it infects all Internet-connected systems on the network. Malware refers to any advanced software designed with the aid of cybercriminals to purloin sensitive data and then damage or destroy computers and computer systems completely or partially. Common malware consists of viruses, worms, Trojans, adware, and ransomware. It is an acronym for 'Malicious Software Program,≈ which includes distinct types of attacks like ransomware, viruses, malware, worms, trojans, and more. Initially, it is installed in the system, which is the target, then collects all the sensitive data, which is beneficial, controls and eventually blocks access to network components, and can destroy sensitive data or shut down the system either partially or completely.

Malware utilizes software program weaknesses and backdoors to gain access to the operating system. Worms can gain access to devices without the user's help. When a user runs an unsafe network or application, an attacker sends a malicious link to that software upon the identical Internet connection. A program that can receive and execute malware containing software programs from the Internet, thereby growing worms. A computer virus is a sort of malicious computer program that, when executed, reproduces itself and inserts its code. When the duplication of code is finished, the malicious code infects other files as well as the programs present in our system. Malicious users download trojans that allow them to manipulate their devices. A Trojan is a type of malicious code or software program that seems valid, but it can exploit our laptop. A Trojan horse, or Trojan, is a type of

code or software that contains malware that looks legal but can take control of your computer. Trojans are developed to harm, steal, disrupt, or conduct other malicious activities on our network. A ransomware attack is a form of malware that denies users access to computer systems or data until they pay a sum of money. When hijackers or malicious actors perform ransomware, criminals attack your computer with malware and keep your computer and data for ransom. The attacker installs software programs on the victim's device and makes use of its computing resources to unknowingly generate cryptocurrency. Malicious actors can benefit from access to unsuspecting user information, along with sensitive information such as passwords and payment details. Malware is a type of malicious software that sets foot into the victim's computer, collects information from their device, and without the user's permission, sends their data to third parties.

The most common kind of malware is malware designed to get into and cause harm to devices without the user's approval. The software program collects sensitive credentials that are sent for advertisement, data collection corporations, or malicious actors for profit. Adware is associated with hooked-up software programs; however, it does not involve the installation of software on the victim's device and mustn't be used for malicious functions, but may be used without the victim's approval and can compromise privacy. Adware is typically made for computers; however, it could also be determined on mobile devices [7]. There are common malware categories and their purposes, as shown in Table 1, and there are the worldwide malware attack statistics from 2015 to the first half of 2022 (in billions) annually, which have been summarized in Fig. 7.

Social engineering attack*:* Victims offer sensitive credentials or accidentally install malicious software on their devices because hackers imitate lawful actors. Using psychology to trick users into making security mistakes or providing important information. Criminals first investigate the planned victim to gather their important and necessary data, including access points and vulnerable safety conditions required to maintain the attack. The attacker then gains the victims acceptance as true and triggers subsequent movements that compromise protection operations together. with exposing touchy facts or granting rights of entry to vital sources. Social engineering is a method that uses human error to gain access to private information, rights, or assets. In cybercrime, "man-hacking "scammers trick unsuspecting users into divulging information, infecting them with malware, or getting access to constrained systems. In baiting, attackers trap users into social engineering traps, normally by promising something attractive, together with gift cards. Victims provide attackers with sensitive information, which includes credentials. A scam is a social attack designed to get the victim to download a link, open software, or download malware. Excusers use a diffusion of tactics and techniques to gain the trust of their target and convince them to provide valuable statistics. Reasoning is a particular social engineering approach that manipulates victims into divulging information. A

pretext is a scenario created by a hazard actor to steal victim information. Under the pretext of an attack, the danger actor asks the victim for certain information, telling them that they need to verify their identity. Phishing includes impersonating a dependent entity in communications such as electronic mail or text messages to obtain sensitive information, including payment card details and passwords.

Trusted employee accounts can also be used to justify attacks targeting individuals through spear phishing. Phishing refers to sending fake emails to many users at the same time, but it is able to be more focused. For example, a common solicitation scheme involves a threat actor calling the victim while pretending to be an official from the IRS. Smishing is a type of social network in which users SMS for attacks. This attack uses fake money to trick people into downloading malware and sharing their sensitive credentials. [12,13]. In smishing, attackers use text messages to trick victims.

In Supply chain attacks, the aim is to spread legitimate programs and malware through the source code, installation process, or software update mechanism. Attackers find unsafe systems, server processes, and various coding methods and use them either to install or update; they also manipulate inception (source) code and hide all malicious data or contents. These types of hackers are particularly serious because the communications from the attacker are signed and verified by trusted senders. In this attack on software, the software dealer does not know whether their software is infected with malware or not. Malicious code executes with the same privileges and trust as infected software. Supply Chain Attack types include manufacturing processes or pipelines, codes signed for a service contract or developer account, malicious code sent as an automatic update of a device or software component, and malicious code already installed on the physical device. The statistics of the software supply chain attack effect in 2021 are shown in Fig. 8.

Table 1. Common Malware [11]

Malware category	Malware Purpose
Virus	Self-replicating software that performs malicious actions on infected computer systems
Trojan Horse	Non-self-replicating software that performs malicious actions on a system while impersonating a legitimate program.
Spyware	Software is commonly embedded in computer systems via browsers that track a computer's activity and report back to a central collection server.
Ransomware	Software restricts access to a system and demands money to restore access.
Keylogger	A hardware device or software that captures every keystroke on a computer and saves it or forwards it to an attacker.

Rootkit	Malicious software is installed and normally hidden from the OS. Rootkits often have more access to the system than the system administrator has.

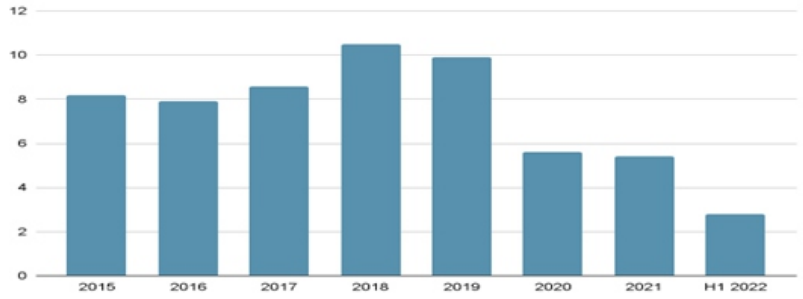
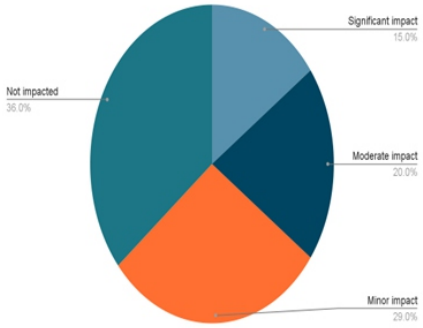
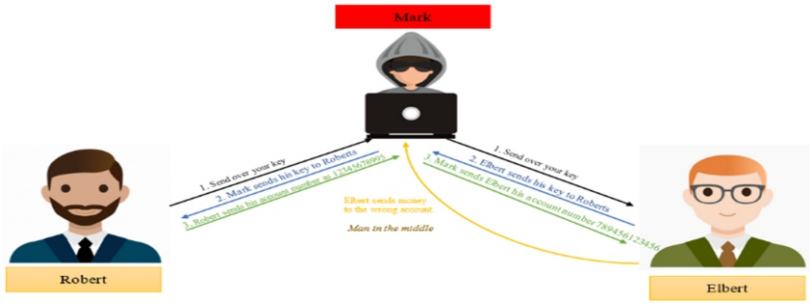


Fig. 7. Annual number of malware attacks worldwide [36]



Man-in-the-Middle (MITM): Man-in-the-Middle attacks involve grabbing communications among two or more victims, such as a user and an application. Fake Wi-Fi allows attackers to detect the activities of victims and collect all the sensitive information, like payment card details and any login credentials. Also known as the "EVIL TWIN≈ attacks, hackers stopped person-to-person Wi-Fi listening by tricking victims into connecting to malicious Wi-Fi networks in the form of human-to-human Wi-Fi eavesdropping attacks. It is almost identical to web security, which involves securing websites and the



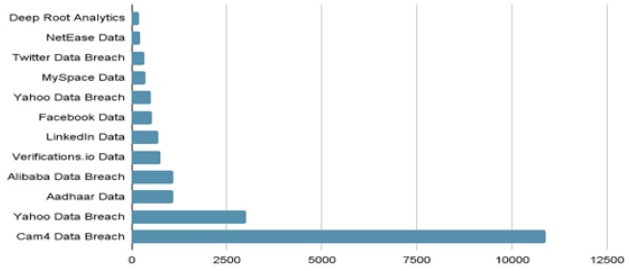
information they contain, but based on mail centers rather than websites. Like web security, email security includes protection against internal threats such as malicious agents and external threats such as hackers and malware. An attacker steals an email address from a legal site, such as a bank, and uses it to trick users into giving sensitive or confidential information or transferring money to the attacker. Domain Name Servers (DNS) redirect users to malicious websites that seem to be legal sites. Attackers can siphon traffic from legitimate sites or steal user credentials. DNS record spoofing is an attack used to redirect online traffic to fake websites that appear to be the intended destination. While there, users are asked to log into their accounts (whatever they think they are), allowing criminals to steal login credentials and other confidential information. In addition, malicious websites are often used to install viruses or malware on users' computers, giving attackers permanent access to those computers and collecting information. Internet Protocol addresses connect users to websites. A hacker could create an Internet Protocol to impersonate a website, causing victims to think that they are interested in that website. IP spoofing is a type of malware attack that hides the actual origin of IP packets to make it difficult for malicious attackers to know where they come from.

Denial of Service (DoS): A denial-of-service attack is a type of attack in which the user network is overloading with a huge quantum of traffic that prevents the system from performing properly. Attacks involving a number of devices are referred to as Distributed Denial of Service attacks. A denial-of-service attack is a type of cyberattack in which an attacker tries to make a device unreachable to the user by disrupting the normal operation of the device. DoS attacks typically work by overwhelming or flooding the target machine until the traffic can be processed, causing a denial of service to the user.

Injection attacks: Injection attacks use various vulnerabilities to inject access to web application code. Attackers enter SQL queries into end-user input channels, such as internet forms. The vulnerability will send the hacker's information to the database and implement the SQL command entered in the request. Most web applications use databases, and these databases are based on a structured query language called SQL, which is unsafe for SQL injection. SQL injection is an attack where malicious code is injected into a string and then analyzed and executed by SQL Server.

If an attacker is vulnerable, the application can inject code. The web server executes the malicious code as if it were part of the program. Entered or injected code can compromise database integrity and/or privacy features, security, and even data integrity. Code injection attacks can break applications that rely on user input to execute. XSS, or Cross-site scripting, is a type of web vulnerability that could allow users to interface with them. interactions with malicious applications. Site script weaknesses often allow a hacker to imitate a victim, compromise users, gain access to user information, perform user-friendly actions, and gain access to user information. If the victim has

privileges over the application, the attacker can have complete control over all operations and data in the application.An attacker can utilize a command injection weakness in load commands to execute the operating system. Shell injection, or OS, is a type of tool for web security that allows a hacker to run a malicious operating system command on the server. The record of selected data breaches in August 2022 is shown in Fig. 10. It represents the count of records disclosed in different data breaches that occurred in August 2022. From the graph the observation indicates that the data breach that released the highest number of records in August 2022 was the Linkedin Data Breach which released over 10,000 million records. The Aadhaar Data Breach disclosed the second highest number of records, equal to 7,750 million records. There were several other data breaches in August 2022, involving millions of records as the following list of data breaches show. The data breaches involved; breach of twitter, yahoo, face book, Alibaba and cam4.



TOOLS FOR DETECTING CYBERCRIME

Besides the physical method, there are also electronic elements. These include software and hardware. A forensic investigation was carried out, whether internal HR documentation, investigations into unauthorized server access, or simply learning new skills. These packages and tools help with audit investigation, hard drive forensics analysis, endpoint detection and response (EDR), risk, electronic discovery, guidance software, compliance, legal software, and commercial investigations.[17] Various tools, including software tools and hardware tools, are used in criminal justice, including:

EnCase©, the international standard for electronic investigation techniques for Criminal Investigation Scientific Research., [7] risk and compliance, e-discovery, and commercial and legal investigations.

EAS (Enterprise Application Software)*:* It is a type of software on the computer that is designed to meet the requirements of not only an individual person. Organization include businesses, schools, consumer groups, charities, associations, and governments. [7]

Forensics: The study of analyzing software to determine whether a crime or theft has happened. [7] It is a source of litigation, judgment, and resolution when companies face copyright infringement, software patent infringement, and trade infringement.

Fast Blog ©: Fast Blog© is a type of software version module. It is a tool designed to control the drives that are read and write and connect these write or read drives via Firewire, SCSI, USB, etc. It ensures the security of files on Windows systems. [7]

DEFENCE METHODS OF CYBER CRIMES

There are numerous methods to locate crime when cybercrimes are experienced. But there are many methods to cover those cybercrimes before they are reused. The use of these cyber defence methods benefits individuals as well as institutions. Hackers are invariably ready for intimate networks. To avoid easy access by hackers, it was necessary to change the settings in the system. The salient technologies that will prevent a bushwhacker from entering the web are Firewall, Honeypot, etc. as shown in Table 2.[7]

Table 2. Cybercrime Defense Methods [7]

NAC	Systems that use security procedures to pierce the network or bias on the tracery.
Air Gap	This system is used to transfer data from one network to another network.
Honeypot	Quarry attackers, analyze attacking types and try to develop appropriate defense devices on the system, especially unsafe devices.
Encryption Systems	Quarry attackers, analyze attacking types and try to develop appropriate defense devices on the system, especially unsafe devices.
Digital Signatures	Digital signatures refer to authorization certificates.
Antivirus	Detection of malware mark and behavior.
DLP	Data Loss Prevention certifies that important information stays within the definite restrictions. Protect information effluence from any hardware or network.
Shorthand	Information is not in an encrypted form, but the data hidden within other messages.
Firewalls	It is a type of network security device that monitors incoming and outgoing network traffic as well as information packets and decides whether to allow entering these packets and block specific traffic based on a defined set
IDS and IPS	Examine the packets over a network, check whether these packets have been allowed to enter in the device.

CASE STUDIES

CASE STUDY -I

Twitter has confirmed that about approx. 5.5 million accounts, along with their email addresses and mobile numbers, were stolen in January 2022 due to a one-day vulnerability on the platform. Vulnerability or defenselessness means that if an unauthorized or bad actor tries to login to an email, they can learn whether that data is linked to an already existing account. Email addresses and mobile numbers associated with 5.5 million accounts continue to be sold on the hacker forum Breach Forum. In a statement, Twitter said it would "immediately notify account holders who can confirm they are affected by this issue." [28] In a previous CS Hub article on July 27, according to the hacker, most of the accounts for sale are "companies, CEOs, celebrities, etc." reported property. "OG" means a Twitter handle consists of arbitrary words, like a nickname, name of person, etc. Twitter suggested that people using "nickname" accounts, such as OG, who may be affected by the breach "keep their identities private" by not adding openly referring to mobile numbers or email addresses to their accounts. Even if no passwords were compromised, then at that time the company said, "Twitter encourages all the users to use 2-factor verification using hardware and software security keys for the protection of our account from unauthorized users or access." [29][30]

CASE STUDY-II

India does not remain silent when we talk about fraud and scam. In 2016, Freedom 251 mobile phone scams, OLX scams, online discount scams, and other major online scams continued to occur over the past two years. Online money transfer is the biggest problem with scams like selling something online. You could say faster than brokers, websites, and apps like OLX or Broker; it has become a major platform for online fraud these days. These include some very low cost or very low-cost portable devices, such as LCD or LED TV cameras. The irony of these ads is that the seller's location appears to be local, even though it is not. The seller is too far away. When the salesperson was called, they claimed he was a busy employee working thousands of miles away. When we call to buy some products, they want money in their account as a prepayment. Some people are tempted to buy cheaper. This is how all sales scams work. This is not the only type of fraud used in India. There has been a rapid increase in fraud during the COVID-19 era, and fraudsters have benefited greatly from the epidemic. The scammers have developed many fraudulent schemes on behalf of the Indian or state governments, and many people have been caught in these schemes. And the job of fueling the fire is being done by social media, which people retweet without thinking. [34] We often see that whenever we receive a fake message on WhatsApp, it says, "return many times", which allows us to guess how many people's fake messages have passed on to us. The image given below shows the news about the Indian government business published by WhatsApp which is completely fake. Social media giants such as

WhatsApp are working hard to prevent the spread of false news and fake news. People also know this through various media, but there is not much difference. This is because of the digital experience. But nothing will happen unless people understand their role in spreading fake news. There was a huge increase from 3,477 cybercrime cases in 2012 to 44,546 cybercrime cases in 2019. In fact, this number nearly doubled in a year, rising from 27,248 in 2018 to 44,546 in 2019(Zheng et al. , 2021).

CONCLUSION

In summary, with the increase in electronic devices and the trust in technology, cybersecurity has become a vital part of everyday life. Understanding the fundamentals of cybersecurity, including the different types of cyberthreats, the attacks used, and the importance of protecting digital assets, is crucial to preventing cyberattacks. The importance of cybersecurity applies to the consequences of a cyberattack that can be devastating for businesses and governments. With limited cybersecurity resources, small-scale businesses are more vulnerable to cyberattacks, and governments face greater threats to national security from cyberattacks. Therefore, it is crucial to monitor network security using effective measures such as firewalls, encryption, and intrusion detection systems. Regular software updates, important data backups, and the best cybersecurity personnel training can be effective in preventing cyberattacks. Consequently, cybersecurity is essential to prevent cyber threats and mitigate the effects of cyberattacks. Understanding the fundamentals of cybersecurity and implementing effective safeguards can help individuals, businesses, and governments protect against the threat of cybercrime and protect the security and integrity of infrastructure, sensitive information, etc.

Conflict of interest

The author declare that they have no conflict of interest

Funding Information

No funding has been used.

Author Contribution

A thorough literature survey has been done of the various types of cybercrimes faced by individuals. The various defense methods that can be used to prevent the cybercrime has been elaborated to make the readers aware of precautions to be taken.

Data Availability statement

The references used in the manuscript has been taken from the renowned platforms like Springer, Elsevier and other internet sources.

Research involving Humans and /or Animals

Not applicable.

Informed Consent

Not applicable

Data Availability

Data sharing not applicable to this article as no data sets were generated or analyzed during the current study.

REFERENCES

Smith, D. J., & Simpson, K. G. L. (2020). *Cyber Security. The Safety Critical Systems Handbook, 269–283.* doi:10.1016/b978-0-12-820258-6.00017-6

Li, Y., & Liu, Q. (2021). *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports.* doi:10.1016/j.egyr.2021.08.126

Sheth, Mrs. & Bhosale, Sachin & Kurupkar, Mr & Prof, Asst. (2021). Research Paper on Cyber Security. 2021.

Frunza, M.-C. (2016). *Cybercrime. Introduction to the Theories and Varieties of Modern Crime in Financial Markets, 207–220.* doi:10.1016/b978-012-801221-5.00015-4

DeTardo-Bora, K. A., & Bora, D. J. (2016). *Cybercrimes: an overview of contemporary challenges and impending threats. Digital Forensics, 119–132.* doi:10.1016/b978-0-12-804526 8.00008-3.

Team, L. (n.d.). classification of cyber crimes. *Lawyersclubindia*. [Online]Available: 700

Okutan, A., & Çebi, Y. (2019). *A Framework for Cyber Crime Investigation. Procedia Computer Science, 158, 287–294.* doi:10.1016/j.procs.2019.09.054.

Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., & Basto-Fernandes, V. (2017). *A Comparison of Cybersecurity Risk Analysis Tools. Procedia Computer Science, 121, 568–575.* doi:10.1016/j.procs.2017.11.075.

Colorossi, J. L. (2015). *Cyber Security. Security Supervision and Management, 501–525.* doi:10.1016/b978-0-12-800113-4.00038-9

John, Jeba Praba. (2016). CYBER SECURITY AND THREATS. 10.5281/zenodo.4383763.

Kaur, J., & Ramkumar, K. . R. (2021). *The recent trends in cyber security: A review. Journal of King Saud University - Computer and Information Sciences.* doi:10.1016/j.jksuci.2021.01.018.

Bendovschi, A. (2015). *Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 28, 24–31.* doi:10.1016/s2212-5671(15)01077-1

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). *Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering.* doi:10.1007/s13369-019-04319-2

Kumar, Sanjeev. (2021). CYBER CRIMES IN INDIA: TRENDS AND PREVENTION. 363.

Vaddi, P. K., Pietrykowski, M. C., Kar, D., Diao, X., Zhao, Y., Mabry, T., º Smidts, C. (2020). *Dynamic bayesian networks based abnormal event classifier for nuclear power plants in case of cyber security threats. Progress in Nuclear Energy, 128, 103479.* doi:10.1016/j.pnucene.2020.103479.

Ficco, M., Choraś, M., & Kozik, R. (2017). *Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. Journal of Computational Science, 22, 179–186.* doi:10.1016/j.jocs.2017.03.025 .

DeTardo-Bora, K. A., & Bora, D. J. (2016). *Cybercrimes: an overview of contemporary challenges and impending threats. Digital Forensics, 119–132.* doi:10.1016/b978-0-12-804526 8.00008-3.

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). *A Survey on Cybersecurity, Data Privacy, and Policy Issues in Cyber-Physical System Deployments in Smart Cities. Sustainable Cities and Society.* doi:10.1016/j.scs.2019.101660.

Katos, V., & Bednar, P. M. (2008). *A cyber-crime investigation framework. Computer Standards & Interfaces, 30(4), 223–228.* doi:10.1016/j.csi.2007.10.003

Von Solms, R., & van Niekerk, J. (2013). *From information security to cyber security. Computers & Security, 38, 97–102.* doi:10.1016/j.cose.2013.04.004.

Khandpur, Rupinder Paul, et al. "*Crowdsourcing cybersecurity: Cyber attack detection using social media.*" Proceedings of the 2017 ACM on Conference on Information and Knowledge Management. ACM, 2017.

Mohammadpourfard, M., Weng, Y., Pechenizkiy, M., Tajdinian, M., & Mohammadi-Ivatloo, B. (2020). *Ensuring cybersecurity of smart grid against data integrity attacks under concept drift. International Journal of Electrical Power & Energy Systems, 119, 105947.* doi:10.1016/j.ijepes.2020.105947

Floyd, D.H.; Shelton, J.W.; Bush, J.E, "Systems and methods for detecting a security breach in an aircraft network," Google Patent, 2018

Taha, Ahmad & Qi, Junjian & Wang, Jianhui & Panchal, Jitesh. (2016). Risk Mitigation for Dynamic State Estimation Against Cyber Attacks and Unknown Inputs. IEEE Transactions on Smart Grid. PP. 10.1109/TSG.2016.2570546.

Von Solms, B., & von Solms, R. (2018). *Cybersecurity and information security – what goes where? Information and Computer Security, 26(1), 2–9.* doi:10.1108/ics-04-2017-0025.

Research Methods for Cyber Security. (2018). *NetworkSecurity, 2018(6), 5.* doi:10.1016/s1353 4858(18)30053-9.

Dibaji, S. M., Pirani, M., Flamholz, D. B., Annaswamy, A. M., Johansson, K. H., & Chakrabortty, A. (2019). *A systems and control perspective of CPS security. Annual Reviews in Control.* doi:10.1016/j.arcontrol.2019.04.011

Powell, O. (2022). Twitter confirms data from 5.4 million accounts has been stolen. Cyber Security Hub.

Umawing, J. (2022). Twitter data breach affects 5.4M users. Jovi Umawing.

Li, Y., Zhang, T., Li, X., & Li, T. (2019). *A Model of APT Attack Defense Based on Cyber Threat Detection. Cyber Security, 122–135.* doi:10.1007/978-981-13-6621-5_10

Reibelt, K., Matthes, J., Keller, H. B., & Hagenmeyer, V. (2020). *Identification and Localization of Cyber-Attacks in Industrial Facilities. 30th European Symposium on Computer Aided Process Engineering, 1747–1752.* doi:10.1016/b978-0-12-823377-1.50292-5

Chen, Dongliang; Wawrzynski, Pawel; Lv, Zhihan (2020). *Cyber Security in Smart Cities: A Review of Deep Learning-based Applications and Case Studies. Sustainable Cities and Society, (), 102655*. doi: 10.1016/j.scs.2020.102655

Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2021). *Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks.* doi:10.1016/j.dcan.2021.07.006

Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., & Basto-Fernandes, V. (2017). *A Comparison of Cybersecurity Risk Analysis Tools. Procedia Computer Science, 121, 568–575.* doi:10.1016/j.procs.2017.11.075

Boughton, N. (2019). *Protecting infrastructure from cyber attack. Network Security, 2019(4), 18–19.* doi:10.1016/s1353-4858(19)30051-0

https://www.statista.com/

https://www.prnewswire.com

Admass, W. S., Munaye, Y. Y., & Diro, A. (2024). *Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 100031*

Prakash, V., Williams, A., Garg, L., Barik, P., & Dhanaraj, R. K. (2022). Cloud-based framework for performing digital forensic investigations. International Journal of Wireless Information Networks, 29(4), 419-441.

De Azambuja, A. J. G., Giese, T., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2024). Digital Twins in Industry 4.0—Opportunities and challenges related to Cyber Security. Procedia CIRP,

121, 25-30.

Jada, I., & Mayayise, T. O. (2023). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management, 100063.

Botta, A., Rotbei, S., Zinno, S., & Ventre, G. (2023). Cyber security of robots: A comprehensive survey. Intelligent Systems with Applications, 18, 200237.