An Investigation of Cybersecurity: Examining Patterns, Hurdles and Solutions

Vipul Badgaiyan[1] Hitesh Ninama[2]
[1]M.Tech Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]School of Computer Science & Information Technology, Devi Ahilya University, Indore (M.P.), India

Abstract — This study examines new trends, problems, and solutions in cybersecurity. This review study has importance because it provides an overview of major cybersecurity types, discusses recent cyberattacks, and analyses the properties, purpose, and motivations of cyberattacks, solutions and specific tools that can be used to mitigate the cyber-attack useful for individuals, businesses, and governments worldwide who want to understand the current state of cybersecurity and how to protect themselves against cyber threats. combination of literature review, and case study analysis is used to write this review research paper. The report begins with a summary of the key results from the Cybersecurity Ventures Report, emphasising the frequency and sophistication of cyberattacks that are becoming more common. Then, a case study is used to evaluate the roles played by the FBI in the USA in battling cybercrime. Prominent recent cyber incidents, such as the 2020 Microsoft Exchange Server and SolarWinds Hack, are examined. By scrutinizing cybersecurity through diverse lenses, the study investigates its fundamental framework, potential remedial measures, and specific tools that hold promise in mitigating cyber threats. It underscores the pivotal importance of devising a comprehensive cybersecurity strategy that encompasses the human element, robust procedural protocols, and cutting-edge technological fortification. The study's conclusion reveals a tapestry of insights into the changing cybersecurity scene and culminates in practical advice for preventing cyberattacks. It emphasises cybersecurity as a major issue that transcends national boundaries and has a big influence on people, businesses, and countries on a worldwide scale, going beyond the bounds of academia.

Keywords: Investigation of Cybersecurity, Cybersecurity Challenges, Cybersecurity Solutions

I. Introduction

According to the Cybersecurity Ventures report, the number of people connected to the internet is expected to reach 7.5 billion by 2030[1], [2], making it more important than ever to address cybercrime. The report also highlights that cyber intrusions and data breaches are on the rise, often due to inadequate training of employees to identify phishing scams. The cost of global cybercrime is anticipated to reach USD 10.5 trillion annually by 2025[1], [2], underscoring the need for businesses and individuals to take cybersecurity seriously. In response to these threats, law enforcement agencies such as the FBI and the Internet Crime Complaint Centre (IC3) in the USA have been established to combat cybercrime and support individuals who report these crimes[3], [4].

Cyber security is a critical concern for businesses, organizations, and individuals in the digital age. Cyber-attacks are deliberate and organized attempts to disrupt or steal data or information from organizations or individuals. Attackers follow specific characteristics to achieve their aims, which include harmonization, organization, enormity, regimentation, scrupulous design, demanding time, and resources, and not being spontaneous or ad hoc[5]. The purpose and motivations of cyber-attacks vary, and the cyber environment of an organization plays a critical role in determining its susceptibility to cyber threats.

Common ways to categorize cyber-attacks include phishing attacks, malware attacks, SQL injection attacks, denial of service or distributed denial of service attacks, cross-site scripting attacks [6]. Cyber attackers include script kiddies, hacktivists, criminal hackers, state-sponsored hackers, insiders, advanced persistent threats, and nation-state actors[6].

The main functions of a cybersecurity framework include identifying, protecting, detecting, responding, and recovering from cyber-attacks[6]. Cybersecurity tools that can help organizations protect against cyber-attacks include firewalls, antivirus software, intrusion detection and prevention systems, encryption, security information and event management systems, penetration testing tools, two-factor authentication, network firewalls, virtual private networks, network access control, distributed denial of service protection, network behaviour analysis, web application firewall, content security policy, SSL/TLS certificates, and web traffic analysis tools [6].

II. Comprehensive Data Synthesis Methodology

1) Data Gathering: An Investigation of Cybersecurity: Examining Patterns, Hurdles, and Solutions was thoroughly studied using records from Cyber Venture, books by reputable writers, peer-reviewed studies, and the FBI IC3 Cyber Crime Report from the USA.
2) Analysis: The landscape of An Investigation of Cybersecurity: Examining Patterns, Hurdles, and Solutions was synthesized using thematic patterns extracted through systematic investigation.
3) Ethical Considerations: Throughout the investigation, the utilization of confidential ethical government data was conducted in accordance with ethical guidelines. Proper attribution has been provided to the original authors of the resources used.

A. The Most Important Findings from the Cybersecurity Ventures Report [1], [2]:

According to the Cybersecurity Ventures report:

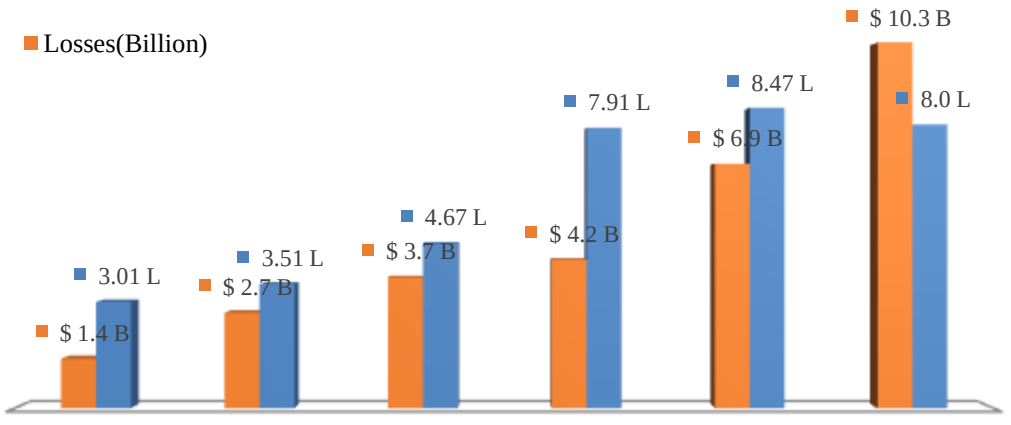
1) 90% of people aged 6 and over will be online by the year 2030. Out of the 8.5 billion individuals on the earth, 7.5 billion will be online, according to that estimate.
2) Data breaches and cyber invasions are a serious concern to all businesses, and they frequently happen because

staff members are not sufficiently taught to spot phishing scams.

3) Failure to learn from past mistakes and take proactive measures to secure digital assets could result in the repetition of similar cyber-attacks.
4) Consumers are plagued by a range of cyber threats including phishing scams, ransomware, and identity theft.
5) Small businesses, including auto dealerships, are especially vulnerable to cyber-attacks as they collect personally identifiable information (PII) from their customers.
6) Cybersecurity Ventures predicts that the world will store a massive 200 zettabytes of data by 2025, including data stored on personal and public devices, cloud data centres, and IoT devices.
7) By 2025, it's predicted that the yearly cost of cybercrime will be USD 10.5 trillion, making it crucial for both enterprises and people to take cybersecurity seriously.
8) Since cybercrimes are not recorded, they are vastly underreported for several reasons, such as embarrassment, worry for one's reputation, and the conviction that law enforcement is helpless to act. Some estimates claim that just 10% of cybercrimes that are committed each year are documented.
9) In 2021, a ransomware attack on a business happened every 11 seconds, and by 2031, Cybersecurity Ventures predicts that there would be a new attack on a client or business every 2 seconds. Following a ransomware attack that blocked access to the company's network and stole its data, CNA Financial, one of the biggest insurance companies in the United States, reportedly paid hackers $40 million, the highest ransom ever.
10) Cybersecurity Ventures estimates that the cost of cryptocurrency-related crimes would increase from an estimated $17.5 billion in 2021 to $30 billion in 2025.
11) Since customers and businesses that have gone digital need to be protected from cybercrime, large organisations spend more than $1 million annually on security. By 2027, it's expected that spending on employee security awareness training will top $10 billion.
12) With 1.5 million cybersecurity job opportunities projected in India alone by 2025, and a major rise in the number of unfilled positions over the years, the shortage of cybersecurity skills has persisted as an issue.

B. Case Study of Roles of IC3 and the FBI in the USA in Combating Cybercrime[3], [4]:

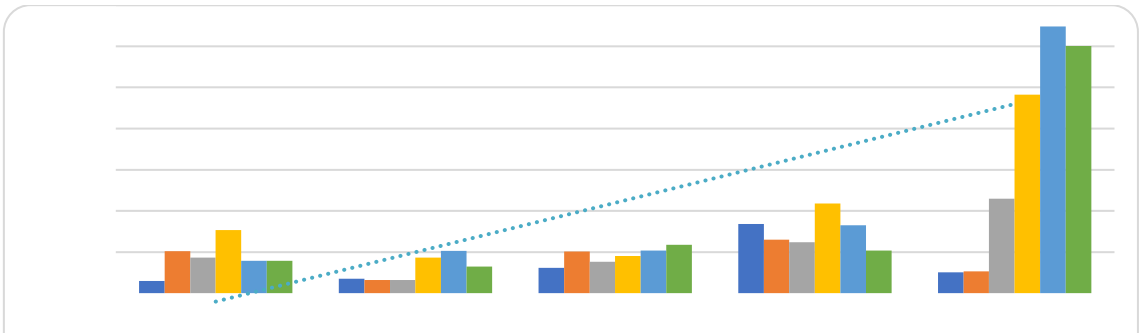
In the US, the FBI is a body in charge of both law enforcement and intelligence. The IC3 was established in May 2000 to deal with complaints concerning cybercrime, including online fraud, intellectual property theft, computer hacking, corporate espionage, and identity theft. As of December 31, 2022, the IC3 has received nearly seven million complaints. To increase public awareness and promote public prevention, the IC3 frequently publishes intelligence reports on trends. An yearly report on the trends influencing the public is also released by the IC3. The accompanying graph shows the total number of complaints and losses reported to IC3 over the preceding six years, from 2017 through 2022. During this time, there were 2,760,044 complaints received by the IC3, and $18.7 billion in losses were documented. In 2021, the IC3 received 847,376 complaints totalling more than $6.9 billion in estimated losses. This is a rise from the previous year, when IC3 received 791,790 complaints with potential losses of $4.2 billion. 2019 witnessed 467,361 complaints and potential losses of $3.5 billion in contrast to 2018, which saw 351,937 complaints and potential losses of $2.7 billion. In 2017, there were 301,580 fewer complaints than in previous years, yet there were still a lot of potential losses ($1.4 billion) documented.



	2017	2018	2019	2020	2021	2022
Losses(Billion)	1.40	2.70	3.70	4.20	6.90	10.30
Complaints(lac(s))	3.01	3.51	4.67	7.91	8.47	8.00

Fig. 1: Complaints and Losses IC3 Report

The reported crime between 2017 and 2022 are compared in the table below in terms of victim losses.



	Extortion	Identity Theft	Personal Data Breach	Non-Payment/ Non-Delivery	Phishing/Vishing/ Smishing/Pharming
2017	14,938	17,636	30,904	84,079	25,344
2018	51,146	16,128	50,642	65,116	26,379
2019	43,101	16,053	38,218	61,832	1,14,702
2020	76,741	43,330	45,330	1,08,869	2,41,342
2021	39,360	51,629	51,829	82,478	3,23,972
2022	39416	32538	58859	51679	300497

Fig. 2: Top 5 Crime Type Comparison Between Years 2017 to 2022 IC3 Report

The volume of complaints and accompanying losses for victims in various age groups are depicted in an infographic in the FBI's Internet Crime Control Centre 2022 and 2021 reports. Age groupings are divided into six categories in the infographic: under 20, 20-29, 30-39, 40-49, 50-59, and 60+. The figure shows that victims under the age of 20 were responsible for 15,782 complaints and $210.5 million in losses. 20 to 29-year-old victims reported 57,978 complaints and losses totalling $383.1 million. The most complaints were filed by people aged 30-39, who accounted for 94,506 victims and $1.3 billion in losses. There were 87,526 and 64,551 complaints from those in the 40–49 and 50–59 age brackets, respectively, as well as losses of $1.6 billion and $1.8 billion. Finally, 88,262 complaints were made by individuals 60 and over who suffered losses totalling $3.1 billion. The infographic only includes complaints that have an age range linked with them, so it's important to keep in mind that there may be other complaints and losses that aren't represented in the statistics.

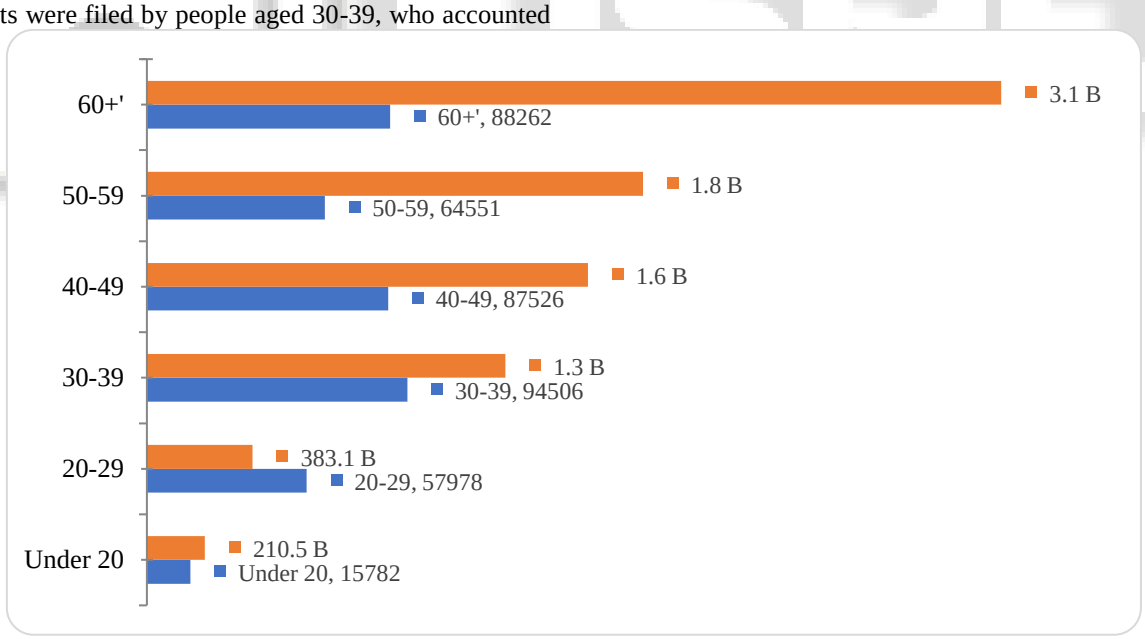


Fig. 3: Age Group Wise Victims as per IC3 report 2022

C. Recent Cyber Attacks [7]:

The Centre for Strategic and International Studies (CSIS) has been monitoring significant cyber incidents targeting governmental organisations, high-tech defence companies, businesses, and economic crimes with losses exceeding $1 million. Their recent report on significant cyber incidents highlights some noteworthy cyberattacks out of those attacks that occurred in February and March 2023 are mentioned below, including DDoS attacks, phishing scams, and cyber espionage operations carried out by state-sponsored and non-state actors. The report covers all significant attacks since 2006. These incidents underscore the persistent and ever-changing nature of cyber threats, requiring sustained effort and investment to counter them effectively. Cybersecurity remains a major concern for governments, businesses, and individuals.

1) Crucial Cyber Attack on March 23[7]

S No	Event Description
1	The website of the French National Assembly was the target of a DDoS attack by Russian hackers for several hours, who claimed that France was supporting Ukraine.
2	German defence company Rheinmetall was the target of a DDoS attack by suspected Russian hackers.
3	In a cyberespionage operation involving numerous attackers, including a Vietnamese espionage cell, a U.S. federal agency was the target.
4	For about a year, a Chinese cyber espionage outfit targeted an East Asian data protection company that provides services to military and governmental organizations.
5	Officials in Estonia claim that during its parliamentary elections, hackers attempted to hack into Estonia's online voting system but were unsuccessful.
6	North Korean hackers targeted cybersecurity research firms in the US in a phishing attempt for cyberespionage.
7	Chinese hackers used malware created by Chinese government hackers in 2008 to attack citizens in Mongolia, Papua New Guinea, Ghana, Zimbabwe, and Nigeria.
8	Using recently created software that was designed to avoid detection, a Chinese cyber espionage outfit targeted governments in Vietnam, Thailand, and Indonesia.
9	Politicians, businesses, and celebrities in the United States and Europe who opposed Putin's invasion of Ukraine were the targets of social engineering initiatives by Russian hackers.
10	A new exploit from a Chinese espionage cell targeting political organizations in Taiwan and Ukraine was found by Slovakian cybersecurity researchers.
11	Russian hackers were responsible for a DDoS assault on Poland's official tax agency website.
12	Between January 2021 and October 2022, 98 serious occurrences that affected the EU transportation sector were listed in a study published by ENISA.

Table 1: Crucial Cyber Attack on March 23 as CSIS

2) Crucial Cyber Attack on Feb 23[7]:

S No	Event Description
1	Exclu is an encrypted communications platform that was broken into & destroyed by the Dutch Police in order to stop criminal organizations' activity. The operation was assisted by police from Italy, Sweden, France, Germany, Eurojust, and Europol.
2	In a phishing effort, Russian hackers used malware to steal information from Ukrainian firms. The malware can capture screenshots, as well as extract files and account information.
3	NATO networks used to transport critical data were subjected to DDoS attacks, according to the pro-Russian hacking organization Killnet. The strike hampered communication between NATO and aircraft sending assistance to a Turkish airbase after an earthquake.
4	A disinformation effort aimed at the Polish public, according to Polish officials. Targets got false information about Ukrainian refugees via email, and officials suggested that these actions might be related to hackers with ties to Russia.
5	Between August and November 2022, an intelligence operation was carried out by the North Korean hacker outfit Lazarus. Targeting industries like chemical engineering, medical research, healthcare, defence, energy, and a research institution, hackers stole over 100MB of data from each victim while going unnoticed. The organization has ties to the North Korean leadership.
6	Russian hackers allegedly started a phishing effort against Latvia's Ministry of Defence, according to officials there. Apparently, the operation was unsuccessful.
7	Italian officials asserted that Acea, a provider of energy for the city of Rome, was the target of a ransomware attack by hackers with ties to Russia.
8	Iranian hacktivists interfered with the state television broadcast of President Ebrahim Raisi's speech during Revolution Day celebrations. "Death to Khamenei" was the hacker cry, and they urged people to participate in anti-government demonstrations.
9	In order to infiltrate target email accounts, an Iranian hacker outfit began an espionage effort against Middle Eastern firms. Researchers assert that Iran's intelligence agencies are connected to the hacking organization.
10	Iranian hackers took down the websites for Bahrain's state news agency and international airport, claiming blame.
11	Hackers attacked Israel's leading technology university, Technion University, with ransomware and demanded 80 bitcoin ($1.7 million USD) to unlock the institution's files. Israeli cybersecurity experts attributed the attack to state-sponsored hackers from Iran.
12	The website of Italy's Revenue Agency (AgenziadelleEntrane) was taken down by hackers, who also used phishing emails to trick users into visiting a fake login page. Within two hours, Italian officials repaired the agency's website.
13	Chinese cyber espionage hackers used a draft EU Commission letter as their initial attack vector in a spear-phishing campaign against government and public sector entities in Asia and Europe.

14	According to the Dutch National Cyber Security Centre, pro-Russian hackers launched DDoS assaults against hospital websites in the Netherlands and other European nations.

Table 2: Crucial Cyber Attack on Feb 23 as CSIS

D. Big hacks[8], [9]:

The globe has recently experienced some of the most damaging cyberattacks in history, underscoring the significance of cybersecurity for safeguarding vital infrastructure and data. The SolarWinds Hack of 2020 and the Microsoft Exchange Server Hack of 2021 were two of the most notable attacks.

1) The on-premises Microsoft Exchange Server software was the victim of a significant cyberattack called the Microsoft Exchange Server hack. The Hafnium hacker collective, supported by the Chinese government, was blamed for the attack. The security of thousands of organisations worldwide was compromised when the hackers used software flaws to access sensitive data [8].
2) The 2020 SolarWinds Hack was an extremely sophisticated supply chain attack on the Texas-based software company SolarWinds. Malicious code was injected into SolarWinds' update system as part of the attack, which was assumed to have been conducted by individuals with the help of the Russian government. The attackers were thus able to intercept communications, steal data from numerous companies, including several U.S. government agencies, and more [9].

E. Purpose and motivations of cyber-attacks[5]:

Cyberattacks have many different goals and objectives, and they go through several procedures:

S No	Purpose/ Motivation	Description
1	Information Obstruction	Attackers aim to block access to critical information, hindering planning and execution.
2	Countering Cyber Security Measures	Attacks challenge international efforts by increasing complexity or evading security.
3	Disrupting Decision Making	Attacks cripple critical areas, causing delays in tactical deployment and life support activation.
4	Denial of Public Services	Attackers disrupt authorized access to public services like banking, transportation, and stock markets.
5	Undermining Public Confidence	Hacking or stealing information erodes public trust in an organization's security.
6	Tarnishing Country's Reputation	Attacks undermine a country's prestige by compromising its networks and competencies.
7	Sabotaging Legal Interests	Attacks aim to disrupt authorized work and processes.

Table 3: Purpose of Cyber Attack

F. Developing a Comprehensive Approach to Safeguarding Digital Assets[10]:

1) Trusted Systems: A trusted system is a computer system that can be trusted to a specified extent to enforce a specified security policy[10].
2) Models for Security: Network security is a scalable and effective method for restricting access and safeguarding digital assets. Security models for organizations span from no security through security through obscurity, host security, and network security[10].

S No	Security Measure	Description
1	No Security	No intentional security measures are in place, leaving digital assets vulnerable to cyber threats.
2	Security by Obscurity	Relying on secrecy as a security measure is unreliable since attackers can discover and exploit vulnerabilities.
3	Host Security	Each host or system within the organization is individually secured with measures like firewalls, antivirus software, and access controls.
4	Network Security	Controls network access to hosts and services, offering scalability and efficiency through measures like firewalls, segmentation, VPNs, and encryption.

Table 4: Security Model

1) Cyber security Goals[11]:

a) Confidentiality: This principle involves protecting sensitive information from unauthorized disclosure or access[11].

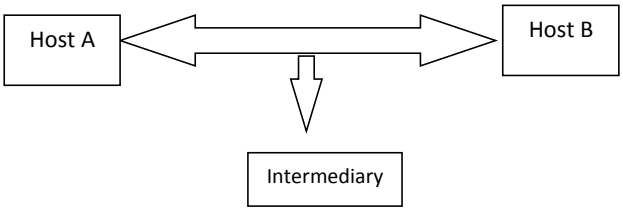


Fig. 4: Confidentiality[10]

b) Integrity: This principle involves maintaining the accuracy, completeness, and consistency of data and system configurations [11].

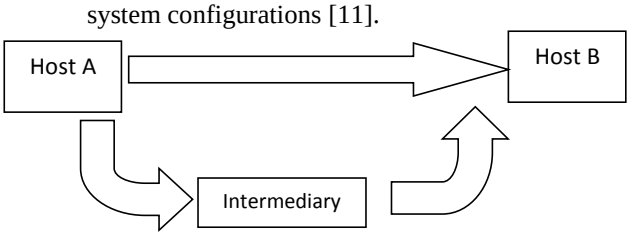


Fig. 5: Integrity[10]

c) Availability: This principle involves ensuring that computer systems and networks are accessible to authorized users when needed [11].

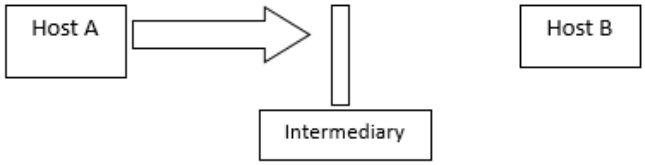


Fig. 6: Availability[10]

d) The CIA triangle and McCumber cube [12]–[14] : Two distinct models are used in the field of information security to comprehend and address various security issues: the CIA triangle and the McCumber cube.

1) The CIA Triangle[12]: The Confidentiality, Integrity, and Availability (CIA) triangle, commonly referred to as the CIA triad, is a fundamental idea in information security. The CIA triangle offers a clear and practical framework for comprehending the core objectives of information security and aids in directing security practises and procedures.
2) The McCumber Cube[12]–[14]: Another paradigm for analysing and rating information security is the W. McCumber Cube. It broadens the CIA triangle and adds other factors to consider in a thorough security analysis. The McCumber Cube extends the standard CIA triad by three additional components:

Elements	Description
Utility	This dimension refers to the usefulness or functionality of the information or system. It assesses whether the information or system serves its intended purpose effectively.
Possession	This dimension refers to the ownership and control of information and resources. It ensures that the right people have proper access to the information.
Authenticity	This dimension verifies the legitimacy and origin of information or communication. It ensures that the information comes from a trusted source and has not been altered or falsified.

Table 5: McCumber Cube components

By considering factors other than the fundamental principles of confidentiality, integrity, and availability, the McCumber Cube offers a more thorough and comprehensive picture of information security. It aids security experts in creating a more thorough security approach by including utility, possession, and authenticity.

	Confidentiality	Integrity	Availability
Utility	Ensures usefulness and functionality of information or system	Ensures accuracy and trustworthiness of information or system	Ensures availability of information and resources when needed
Possession	Ensures proper ownership and control of information and resources	Ensures proper ownership and control of information and resources	Ensures proper ownership and control of information and resources
Authenticity	Ensures information comes from a trusted source and has not been altered or falsified	Ensures information is not altered or falsified and comes from a legitimate origin	Ensures information is available from a trusted source and has not been altered or falsified

Table 6: McCumber Cube components With CIA

2) Enhancing Security through a Robust Policy[10]:

Implementing effective security-management practices necessitates the establishment of a well-defined security policy. While creating a comprehensive security policy can be challenging, it plays a vital role in ensuring adequate security measures. A strong security policy typically encompasses four crucial elements:

S No	Security Policy Consideration	Description
1	Cost-Effectiveness	Evaluating the financial and operational implications of security implementation is essential to ensure an affordable approach that aligns with the organization's resources.
2	Functional Approach	Defining the mechanisms and strategies employed to provide security is a core aspect of the policy. This includes outlining the technologies, procedures, and protocols utilized to safeguard assets effectively.
3	Cultural Alignment	A successful security policy considers the organization's culture, considering the expectations, work styles, and beliefs of its members. This enables the policy to be better accepted and integrated into daily practices.
4	Legal Compliance	Adhering to relevant laws and regulations is crucial to maintain a lawful and ethical security environment. The policy should align with legal requirements to mitigate potential legal issues.

Table 7: Security Policy Consideration

Once a security policy is in place, the following steps contribute to its effective implementation:

1) Clear Communication: Thoroughly explain the policy to all stakeholders involved, ensuring they understand its purpose, guidelines, and implications[10].
2) Role Clarification: Clearly define the responsibilities and roles of individuals or teams involved in security management, promoting accountability and clarity[10].

3) Simplified Language: Utilize straightforward and easily understandable language in all communication regarding the security policy, facilitating comprehension and compliance[10].
4) Accountability Measures: Establish mechanisms to hold individuals accountable for their adherence to the policy, fostering a sense of responsibility and ownership[10].
5) Flexibility and Review: Incorporate provisions for exceptions and periodic reviews to accommodate evolving security needs and adapt to changing circumstances effectively[10].

3) Cyber attackers [6]:

Individuals or groups who engage in malicious activities on the internet with the intention of gaining unauthorized access to computer systems or networks, stealing data, causing damage, or other illegal purposes. They can be classified into different categories based on their level of expertise, motivations, and techniques. Here are some common classifications of cyber attackers:

S No	Type	Description
1	Script Kiddies	Individuals with little to no technical knowledge who use pre-made tools to launch attacks. They target easy targets and aim to prove their hacking skills.
2	Hacktivists	Attackers motivated by political or social issues who use hacking to promote their cause. They target government or corporate websites, deface them, or steal sensitive information for exposure.
3	Criminal Hackers	Attackers motivated by financial gain who employ sophisticated techniques to steal credit card numbers, personal information, or other valuable data. They may use ransomware for extortion.
4	State-Sponsored Hackers	Attackers employed by governments or intelligence agencies who engage in hacking to gain a strategic advantage. They may conduct cyber espionage, sabotage, or other malicious activities.
5	Insiders	Employees or contractors who have access to sensitive information and abuse their privileges for personal gain or to cause damage. They may steal trade secrets, customer data, or other confidential information.
6	Advanced Persistent Threats (APTs)	Highly skilled attackers who use sophisticated techniques to penetrate an organization's defences and remain undetected. They employ social engineering, zero-day exploits, and other advanced methods to steal data.
7	Nation-State Actors	Government-sponsored groups that engage in cyber operations to further their national interests. They target critical infrastructure, military systems, or political organizations of other countries.

Table 8: Cyber attackers Type

4) Security Paradigms:

Least Privileges, Perimeter vs. Layered, and Proactive vs. Passive Defense[12]:

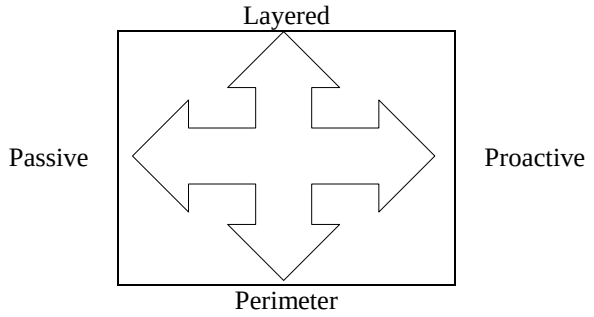


Fig. 7: Security Approach Guide [12]

a) Least Privileges: According to the least privilege concept, users or services should only be given the rights necessary to carry out their duties. It seeks to lessen unauthorised access and restrict the harm caused by insider threats. Organisations can reduce the effect of security incidents by using this concept, which guarantees users have only the access they require.

b) Perimeter vs. Layered Security: Perimeter Security Approach focuses on securing the network perimeter with firewalls, proxy servers, and password policies, making unauthorized access difficult. However, it may neglect internal system security. Layered Security Approach goes beyond perimeter security, securing individual systems within the network, including servers and workstations. It employs network segmentation to isolate segments and enhance defence against various threats.

Security Approach	Focus	Key Features
Perimeter Security	Securing the network perimeter, to prevent unauthorized access	1. Firewalls and proxy servers
		2. Password policies
		3. Restricted external access
Layered Security	Extending security measures to internal systems within the network	1. Securing individual systems (servers, internal systems within the Network segmentation)
		2. Multiple layers of security for various threats

Table 9: Perimeter vs. Layered Security

c) Proactive vs. Passive Defence: Proactive Defence focuses on preventing attacks by identifying and mitigating risks beforehand. Measures include intrusion detection systems, regular security

assessments, threat intelligence, and strong security policies. Passive Defence is reactive and responds to incidents after they occur. It involves incident detection, response plans, investigations, and reporting to minimize impact.

Security Approach	Focus	Key Measures
Proactive Defence	Preventing attacks before they occur	Intrusion detection systems (IDSs)
		Regular security assessments and audits
		Advanced threat intelligence and monitoring tools
		Strong security policies and procedures
Passive Defence	Reacting to security incidents after they have occurred	Incident detection
		Incident response plans
		Forensic investigations
		Incident reporting

Table 10: Proactive vs. Passive Defence

d) Hybrid Approach: In practice, network security often adopts a hybrid approach, combining elements from both perimeter and layered security approaches. Networks may have both passive and proactive defence measures. The most desirable hybrid approach is a layered paradigm with a dynamic nature, combining strong perimeter security measures with robust security measures for individual systems within the network. This approach acknowledges the importance of securing the perimeter while also addressing internal vulnerabilities, and emphasizes a proactive defence strategy to prevent attacks before they occur.

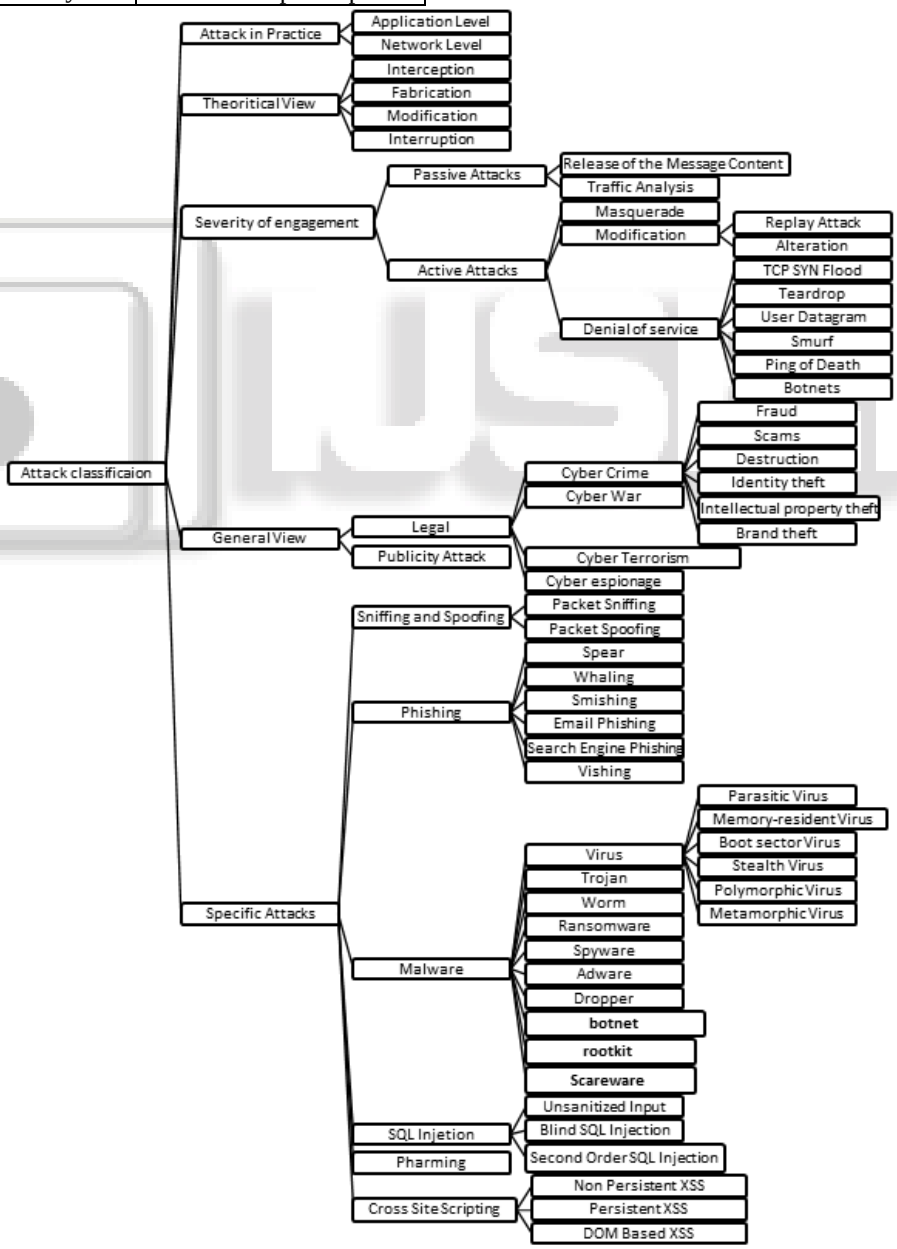


Fig. 8: Cyber Attack Classification

G. Cyber Attack classification[5]–[7], [10], [11], [15]–[36]:

The systematic classification and study of various forms of hostile behaviour directed at computer systems, networks, and digital assets is referred to as "cyberattacks, classification." Figure 7 will categorise cyberattacks as follows:

1) The Practical Side of Attacks[10]:

a) Application-level Attacks[10]: Application-level assaults take place at the application level, where the attacker focuses on certain apps to gain unapproved access, modify data, or impair their functionality. The integrity, confidentiality, or availability of the targeted application or its related data are all targets of these assaults. Examples & Case Studies
   1) stealing credit card details from an internet form
   2) altering message content to affect a transaction amount

b) Network-level Attacks[10]: Network-level assaults concentrate on reducing or preventing a computer network's functionality in various ways. These attacks aim at the network infrastructure itself, and by granting unauthorised access to critical data, they may pave the way for future application-level attacks. Attack Methods and Effect:
   1) Slowing down or halting the normal functioning of a computer network
   2) Exploiting vulnerabilities in network devices or protocol.

2) Theoretical Concepts[10]:

Numerous attacks put the confidentiality, integrity, and availability of resources at risk in the context of security principles. Four categories—interception, fabrication, alteration, and interruption—can be used to group these attacks.

a) Interception[10]: The term "interception" describes when a person, programme, or computer-based system gains access to a resource without authorization. It entails tasks like copying data or programmes and keeping track of network traffic. Attacks that intercept data have the goal of obtaining sensitive information or interfering with an application's normal operation.

b) Fabrication[10]: Fabrication is the process of creating phoney or unlawful items using a computer system. To trick the system or users, an attacker may create false data or add fictitious records to a database. Attacks that change data in an effort to deceive users or take advantage of flaws in the system are called fabrication attacks.

c) Modification[10]: Attacks against databases, messages, and other data sources are primarily focused on changing their contents or values. Attackers may alter data to affect transactions, alter records, or make unauthorised system changes. These attacks have a direct impact on the accuracy of the data and may have serious repercussions.

d) Interruption[10]: Attacks that cause disruptions interfere with a resource's usability or availability. They inconvenience or hurt users by making the resource lost, inaccessible, or unusable. Hardware issues, wiping crucial files or programmes, or performing Denial-of-Service (DoS) attacks are a few examples of interruption attacks.

3) Severity of engagement:

a) Passive Attacks[10]: Eavesdropping or monitoring data transfer without changing the original message's content characterises passive attacks. The aim of passive attacks is information gathering while avoiding detection. Since passive attacks are more difficult to identify, prevention is a major strategy for dealing with passive attack.
   1) Release of Message Contents[10]: When unauthorised parties access private information that was meant for specific recipients, the contents of messages are released. The disclosure of message contents can be prevented with the aid of security measures like encryption. However, attackers might try to use traffic analysis to spot trends in encoded messages and learn more about the communication being carried out.
   2) Traffic Analysis[10]: As a subset of passive attacks, traffic analysis examines patterns in encoded signals to infer details about the communication. An attacker may learn details about the communication by comparing and analysing similarities and trends across a large number of messages, jeopardising its confidentiality.

b) Active Attacks[10]: Modifying the original message or sending fake messages are examples of active attacks. Active attacks, in contrast to passive attacks, call for alterations to the message's content. Active attacks can be recognised with effort, even though it is difficult to avoid them, and recovery mechanisms can be put in place.
   1) Masquerade Attacks[10], [11]: Masquerade assaults happen when an unauthorised person impersonates someone else to trick their target. In order to gain unauthorised access or deceive other users, this entails taking on the identity of an authorised user or system. Masquerade attacks frequently contain additional active attack types, including recording or replaying authentication steps to get unauthorised access.
   2) Replay Attacks[10], [11]: Replay attacks entail collecting and resending a series of events or data units. For instance, an attacker might intercept a request for a money transfer and replay it to the bank of the recipient, causing unauthorised duplicate transactions. Attacks that use replays take advantage of holes in message authentication and verification systems.
   3) Alteration of Messages[10]: The term "message alteration" describes unauthorised changes made to the original message's content. Attackers may alter the message's beneficiary, quantity, or other important details to influence the intended action or deceive the recipient. This kind of attack jeopardises the communication's honesty and dependability.
   4) Denial-of-Service (DoS) Attacks[6], [10], [11], [37], [38]: Attacks known as denial-of-service (DoS) or

distributed denial-of-service (DDoS) are malicious actions intended to disable a host's internet connections and prevent authorised users from accessing it. These attacks send an overwhelming amount of requests or bandwidth to the target server, causing it to crash or stop responding. DoS assaults normally come from a single source, whereas DDoS attacks are coordinated by a large number of infected machines (botnets). DoS attacks can be carried out for a variety of reasons, from self-gratification to harming an organization's reputation. Loss of client confidence and revenue are just two of the negative effects that these attacks may have.

S No	Attack Type	Description
1	TCP SYN Flood Attack	Exploits the buffer space during a TCP session initialization handshake by flooding the target system with connection requests.
2	Teardrop Attack	Sends fragmented data packets to the target system, targeting flaws in TCP/IP fragmentation reassembly, causing crashes.
3	User Datagram Protocol (UDP) Flood	Floods the target system with a large number of UDP packets, overwhelming network and security elements.
4	Smurf Attack	Overwhelms a target network with traffic by sending ICMP echo requests to broadcast IP addresses.
5	Ping of Death Attack	Sends oversized IP packets to a target system, causing buffer overflows and crashes when reassembled.
6	Botnets	Networks of compromised systems used to carry out DDoS attacks, overwhelming target systems with coordinated traffic.

Table 11: Sources of Denial-of-service attack

4) General View

a) Legal Attack[5], [10]: Legal classification is a technique for classifying cyberattacks based on legal definitions. Legal Attack four main sub categories: cybercrime, cyberespionage, cyberterrorism, and cyberwar.

1) Cyber Crime[10]: Cybercrime is defined as any crime in which a computer is either the tool or the intended victim. Computers are used by cybercriminals to carry out their crimes because of their anonymity and storage capacity. Inadequate user education and weaknesses in the operating system might also contribute to cybercrimes.

S No	Attack Type	Description
1	Fraud	ATMs, checks, credit cards, electronic stock certificates, letters of credit, electronic stock certificates, electronic checks, and electronic stock certificates are just a few of the items that are frequently used in modern fraud efforts to take advantage of certain features. Attackers attempt to deceive individuals or organizations in order to get illegal access to cash or private information. This could entail dishonest tactics like identity theft, phishing scams, or fiddling with financial documents for personal gain.
2	Scams	Scams come in various forms, including those that include the sale of services, auctions, multi-level marketing schemes, commonplace commodities, and business opportunities. People are convinced to donate money in exchange for spectacular returns, but they ultimately lose it. The Nigerian scam is an illustration of a typical fraud in which people who receive emails from Nigeria (and other African countries) are convinced to deposit money into a bank account in exchange for the promise of big earnings. People who fall victim to these scams suffer significant financial losses.
3	Destruction	Such assaults are brought on by resentment of some kind. For instance, although terrorists normally target larger targets, dissatisfied employees frequently target their own workplace. During an attack in 2000, authorised users of well-known Internet sites like Yahoo!, CNN, eBay, Buy.com, Amazon.com, and E*Trade were unable to log in or access them. These attacks caused inconvenience and interruption for the users.
4	Identity theft	Rather than stealing from legitimate users, attackers assume their identities. The intention is to conduct fraud or make money by using someone else's identity. Attackers may get passwords, bank account access, or credit cards in another person's name. They use the stolen identity as soon as they have it until it is detected. Identity thieves cause serious financial and reputational harm to their victims.
5	Intellectual property theft	Theft of intellectual property includes taking software, databases, digital music and movies, electronic books and papers, trade secrets, and more. In order to gain a competitive edge, damage enterprises, or make

		money from the sale of stolen intellectual property, attackers target valuable intellectual property. Such theft can cause financial losses as well as harm to a company's brand and ability to innovate.
6	Brand theft	Software, databases, digital music and movies, electronic books and papers, trade secrets, and other types of intellectual property are all included in intellectual property theft. Attackers target priceless intellectual property in order to obtain a competitive advantage, hurt businesses, or profit from the sale of stolen intellectual property. Such theft can impair a company's reputation and innovation capacity in addition to causing financial losses.

Table 12: Criminal Attack

2) Cyber Espionage[6]: Cyber espionage is the illegal activity of getting confidential information from people, organisations, or governments without their consent. Cyber espionage, commonly referred to as cyber spying, may involve experts operating from remote locations or the hacking into computer systems by amateur programmers and hackers or traditional spies.
3) Cyber Terrorism[6]: Cyberterrorism is the use of online attacks for terrorist purposes, such as the widespread disruption of computer networks by computer viruses. Many governments across the world have created laws and policies to combat cyber terrorism because it can pose a severe threat to national security.
4) Cyber War[6]: Cyber War is the act of one nation state infiltrating the computer or network of another nation in order to disrupt or cause damage. Attacks on military networks, government infrastructure, or vital infrastructure, such as power grids and water treatment facilities, can all be part of cyberwarfare. Cyber warfare is a tactic that governments may employ for espionage, sabotage, or even as a weapon of war. Cyberwarfare can have significant repercussions on the economy, politics, and society.
5) Publicity Attack[10]: Attackers who want their names to appear in newspapers and on television news channels do publicity attacks. According to historical evidence, these attackers are typically not seasoned felons. These individuals, who use a fresh strategy to attack computer systems, include university students and workers of huge corporations. Attacking a website and damaging (or defacing) its Web pages is one type of PR attack. The US Department of Justice's website was the target of one of the most well-known of these attacks in 1996. Two years later, the New York Times homepage was also infamously vandalised.

5) Specific Attacks[10]:

a) Sniffing and Spoofing[10]: Computers communicate with one another on the Internet by sending and receiving packets, or tiny collections of data. Attackers concentrate on these packets as they move over the Internet from the source computer to the destination computer. Attacks often fall into one of two categories: packet sniffing, also known as snooping, or packet spoofing. These assaults, which target the Internet Protocol (IP) used for communication, are also known as IP sniffing and IP spoofing.

S No	Attack Type	Description
1	Packet Sniffing	Attacker watches conversational packets in a passive manner without taking control of the conversation. Attacker needs access to a computer that handles the traffic, like a router. Sniffing can be avoided by taking precautions like encoding or encrypting the data.
2	Packet Spoofing	Attack in which a fake source address is used to deliver packets. Unknowingly, the recipient replies to the counterfeit address. The reply might be intercepted, a DoS attack could be launched, or a fake address could be used to trick the recipient.

Table 13: Sniffing and Spoofing

b) Phishing[6], [31], [32], [39], [40]: One of the most prevalent types of cyberattacks is phishing, in which the attacker poses as a reliable entity to gain sensitive information like usernames, passwords, and credit card details. These attacks are frequently carried out using modern tools like emails and phone calls. We will talk about the most common phishing attack types in this section.

S No	Attack Type	Description
1	Spear Phishing	Attackers using targeted phishing techniques to target particular people or organizations, such as system administrators at a business.
2	Whaling	High-level executives, including CEOs and CFOs, are the target of a highly focused phishing campaign that sends misleading emails with fake information.
3	Smishing	Phishing attacks using text messages or SMS are carried out by sending victims messages asking them to click on links or submit personal information.
4	Email Phishing	A common form of phishing in which bulk emails are sent to many email addresses, generally alleging that the recipients' accounts have been compromised and enticing them to click on the offered links.

5	Search Engine Phishing	Search engine results are manipulated to make harmful websites appear first. After that, victims are routed to various websites, where they could be asked for sensitive data.
6	Vishing	Phishing attacks over the phone use social engineering strategies to trick victims into divulging personal information and are frequently directed at bank accounts.

Table 14: Sniffing and Spoofing

c) Malware[5], [6], [15], [34]: Malware is a term used to describe software that is intended to interfere with the proper operation of equipment like computers, mobile phones, and servers. The user may unintentionally install it by downloading infected files or clicking on malicious links, among other methods. Malware can serve a variety of functions, such as gaining unauthorized access, monitoring users, wreaking havoc, or stealing money from unwitting targets. Here are a few prevalent malware attack types.:

1) Virus[10], [15]: A virus is a bit of malicious programmed code that affixes to healthy programmed code and spreads when the healthy program is executed. On the same computer or across a network, viruses can spread to other program. Computer and network systems can sustain damage, but effective backup and recovery strategies can lessen the effects. Based on their behavior and characteristics, viruses can be divided into various types. These are the categories:

S No	Virus Type	Description
1	Parasitic Virus	The most prevalent kind of virus attaches to executable files and spreads by infecting more executable files. When a virus-infected file is run, it spreads to further files and continues to replicate.
2	Memory-Resident Virus	The executable programs that are run while the virus is present in memory are infected by this form of virus, which attaches itself to a specific location in the computer's memory. Even after the first infection, it continues to operate in the memory, giving it the ability to spread to other running programs.
3	Boot Sector Virus	The master boot record (MBR) or boot sector of a storage device, such as a hard drive or floppy disc, is infected by boot sector viruses. When the infected disc is accessible, the virus can spread to other discs or computers. They become active when the machine turns on and infect the boot process.
4	Stealth Virus	Stealth viruses are created to evade detection by antivirus software and other systems. It is challenging for antivirus programs to recognize their presence since they frequently use a variety of evasion strategies, such as intercepting system calls or changing the outcomes of file system operations.
5	Polymorphic Virus	With each infection, polymorphic viruses have the capacity to alter their coding or signature. This implies that each time the virus replicates, it creates a fresh copy of itself that has undergone minor changes. As a result, antivirus software that relies on particular signatures or patterns will have a harder time detecting the virus.
6	Metamorphic Virus	Similar to polymorphic viruses, metamorphic viruses take it a step further by rewriting their whole source code during each replication. This indicates that the virus not only alters its signature but also its internal structure and behavior, making it much more challenging to identify and examine.

Table 15: Types of virus

d) Worm[6], [10], [15]: Worms replicate themselves without modifying other programs. They consume system resources, often leading to slow or halted computer or network operations. Unlike viruses, worms do not perform destructive actions themselves.

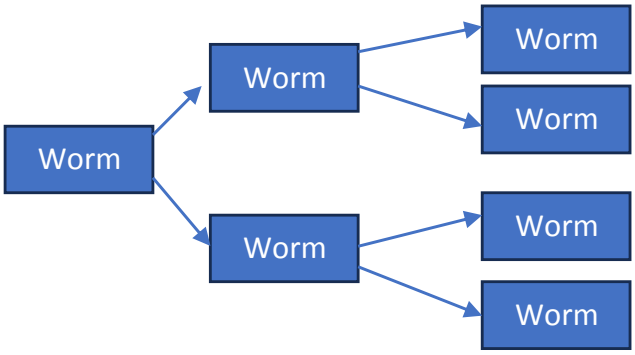


Fig. 9: Worm

e) Trojan[6], [10], [15]: A Trojan is a hidden piece of code that appears to be legitimate but has a malicious purpose. It aims to reveal confidential information to an attacker. Trojan horses can be disguised as harmless files or applications, tricking users into executing them.

f) Ransomware[6], [10], [15]: It is a type of malware that encrypts the victim's files, making them inaccessible, and then demands a ransom payment in exchange for the decryption key. WannaCry and

Maze ransomware are examples of well-known ransomware attacks.

g) Droppers [6], [10], [15]: Droppers are applications used to infect computers with viruses. They may go undetected by virus-scanning software since they don't contain dangerous code themselves. Droppers can also download updates to virus software on compromised systems.

h) Adware [6], [10], [15]: Adware is software that displays advertising banners or pop-ups while a program is running. It is often downloaded automatically while browsing websites and can be viewed as intrusive or unwanted.

i) Spyware [6], [10], [15]: Spyware is set up on a user's computer or web browser to collect information about their online activities. After covertly capturing user behavior, it discreetly transfers the information to a remote user. Additionally, spyware can use the internet to install dangerous software. It is similar to adware in that it commonly gets installed by accident together with other freebie programs.

j) Scareware[15]: Scareware is fake antivirus software that scans a user's device for malware and security threats in an effort to get them to pay to have it removed.

k) Botnet[15]: A group of computers that communicate online is referred to as a botnet, or robot network. A command and control center employs them to conduct distributed denial-of-service (DDoS) assaults (see below), send spam, and engage in other illicit activities.

l) Root kit[15]: A rootkit can be used by an attacker to get root or privileged access to a computer or computer network as well as potentially other devices connected to the same network if they have administrator-level access to the system.

m) SQL Injection[6], [21]–[27], [41]–[49]: SQL injection (SQLi) is an attack technique that targets SQL databases. It occurs when an attacker manipulates SQL queries used to interact with a database, typically through user input on a web application. If the application fails to properly validate or sanitize the user input, the attacker can inject malicious SQL code, potentially gaining unauthorized access to the database or manipulating its contents. SQL injection attacks can lead to data breaches, data manipulation, unauthorized data access, and even complete compromise of the underlying system.

S No	SQL Injection Type	Description
1	Unsensitized Input	Attackers exploit input fields that lack proper sanitization or validation by the application. They inject specially crafted input, such as SQL commands or malicious data, to manipulate the SQL queries executed by the application. This can lead to the retrieval of sensitive data or the execution of unauthorized actions.
2	Blind SQL Injection	Attackers rely on inference and analysis of application responses to gather data, without directly retrieving information from the database. By injecting specific SQL payloads and analyzing the application's behavior (e.g., response time, error messages), the attacker deduces information about the database structure, extracts data, or modifies the application's behavior.
3	Second Order SQL Injection	Attackers exploit the improper handling of user-supplied data stored in the database. They inject malicious input that is later used to construct SQL queries. This type of attack bypasses input validation and security measures, enabling the attacker to execute unauthorized SQL commands and potentially compromise the database.

Table 16: Types of SQL Injection

6) Pharming (DNS Spoofing)[10]:

Pharming is an attack that tricks the Domain Name System (DNS) to lead users to phony websites. It was formerly known as DNS spoofing or DNS poisoning. The DNS system converts human-readable domain names, such as www.example.com, into computer-understandable IP addresses, such as 192.168.0.1. In a pharming attack, the attacker hacks a DNS server and changes a domain name's legitimate IP address to one of their own. When users seek to access the legitimate website as a result, they are instead sent to the attacker's phony website.

7) Cross-Site Scripting (XSS)[6], [17]–[20], [27]:

Cross-Site Scripting (XSS) is a type of attack where malicious scripts are injected into web applications to run in the victim's web browser or scriptable application. It occurs when an application fails to properly validate or sanitize user input, allowing an attacker to inject and execute malicious scripts within the context of a trusted website. XSS attacks can have severe consequences, including the theft of sensitive information, session hijacking, and unauthorized access to user data.

S No	XSS Attack Type	Description
1	Reflected XSS or Non-Persistent XSS Attacks	In this kind of attack, a malicious script is added to the URL as a query parameter. Usually, the attacker provides the link by email (phishing) or fools the victim into clicking on it. The script is executed by the victim's browser when they click the link, injecting the script into the web page. The injected script has the ability to

		steal private data from the victim or act in the victim's place within the application.
2	Persistent XSS Attacks (Type 2 XSS)	This kind of attack involves injecting a malicious script that is kept on the server of the online application that is at risk. Other people that visit the hacked website are subsequently served the script. These users' browsers run the malicious script when they load the page containing it, which could result in data theft or unauthorized actions.
3	DOM-Based XSS Attack	The client-side scripts of the web application are vulnerable to this kind of assault. The attacker manipulates the Document Object Model (DOM) and inserts malicious scripts into the target browser by taking advantage of vulnerabilities in the application's own client-side scripts. DOM-based XSS, in contrast to other XSS attacks, relies on client-side code vulnerabilities rather than server-side injection.

Table 17: Types of XSS Attack

H. Taxonomy of attack that Beaches Security Goals[11]:

The presentation of attacks that violate security objectives is provided below. Under the integrity goal, attacks including alteration, disinformation, replaying, and repudiation seek to undermine the accuracy and validity of data. Attempts to compromise private data using snooping, sniffing, traffic analysis, and the publishing of message content are a few examples of confidentiality-focused assaults. Availability is threatened by both denial of service (DoS) attacks and distributed denial of service (DDoS) attacks, which spread their effects over multiple systems. Recognizing certain attack types and taking appropriate action are crucial for maintaining the integrity, confidentiality, and availability of digital systems and data.

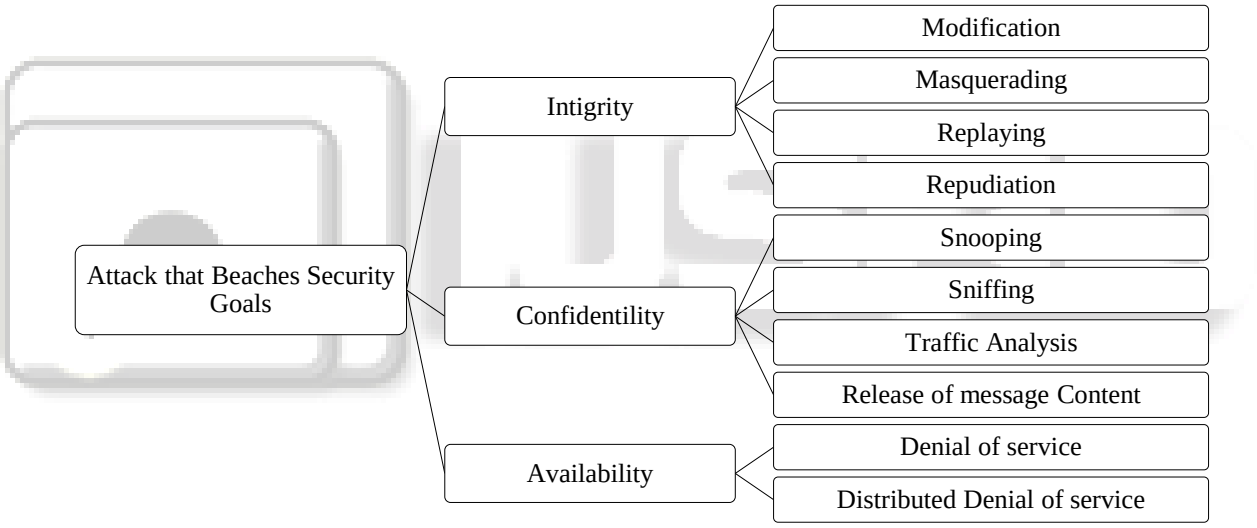


Fig 10: Attack that Beaches Security Goals

I. Cyber environment of an organization[35]:

The safeguarding of data is essential in everyone's daily life. Confidentiality, integrity, and availability are the three main objectives of information security. Some recommendations for addressing information security issues include ensuring self-efficacy, ensuring a favourable understanding of the information security environment, and ensuring that all levels of the company apply security regulations to their daily actions.

Fig 11: Cyber environment of an organization

The picture emphasises how important it is to maintain information's accessibility, confidentiality, and integrity across the cyber environment in order to safeguard the security of the organisation. It also draws attention to the risks and dangers that could endanger the organization's security, such as malware, social engineering, cyberattacks, and human error. The example emphasises the need for a comprehensive and integrated information security policy that covers the various risks and threats that can affect the organisation and considers all aspects of the cyber environment.

J. Cyber security tools [6], [50]:

Cybersecurity tools are software or hardware technologies designed to help organizations prevent, detect, and respond to cyber threats. Some common cybersecurity tools include:

1) Essential Cybersecurity Tools for Safeguarding Computer Systems and Networks[6], [10], [11], [51]–[58]:

An essential piece of software or hardware that helps defend against common online threats and improves the overall security of computer systems and networks is referred to as a fundamental cybersecurity tool. Examples of fundamental cybersecurity tools include the following:

S No	Firewall Type	Description
1	Packet Filters	Examine individual packets by analysing attributes like source/destination IP addresses, protocol types, and port numbers.
		Decide whether to allow or discard packets based on predefined filtering rules.
		Operate at the network and transport layers of the network stack.
		Generally fast in processing packets.
		Configuring packet filters correctly can be challenging.
		May lack support for authentication.
2	Application Gateways (Proxy Servers)	Act as intermediaries between internal users and external hosts.
		Control the flow of application-level traffic and provide enhanced security.
		Request information about the remote host and authenticate the user when a connection is initiated.
		Establish a connection with the remote host on behalf of the user and relay packets between them.
		Offer improved security compared to packet filters.
		Managing multiple connections can introduce additional overhead.

Table 18: Types of Firewall

a) Antivirus Software[6], [10]: Malicious software, such as viruses, worms, and trojan horses, is found, stopped, and eliminated by antivirus software. To keep the system safe, it checks files and programmes for known malware signatures and behavioural patterns.

b) Firewalls[6], [10]: A firewall acts as a protective barrier between a company network and the outside world, usually the Internet, and is an essential part of network security. Its main job is to secure the network against attacks and prevent unauthorised access. Firewalls are essential for protecting sensitive information within corporate networks and reducing the possibility of external threats like viruses and worms inflicting damage. Packet filters and application gateways (sometimes known as proxy servers) are the two main categories of firewalls. By permitting authorised traffic to pass through while preventing or discarding unauthorised or suspect traffic, firewalls enforce security policies. They make sure internal data is secure and defend

against potential outside attacks. In order to protect sensitive data and corporate networks, firewalls serve as a crucial part of the network security infrastructure.

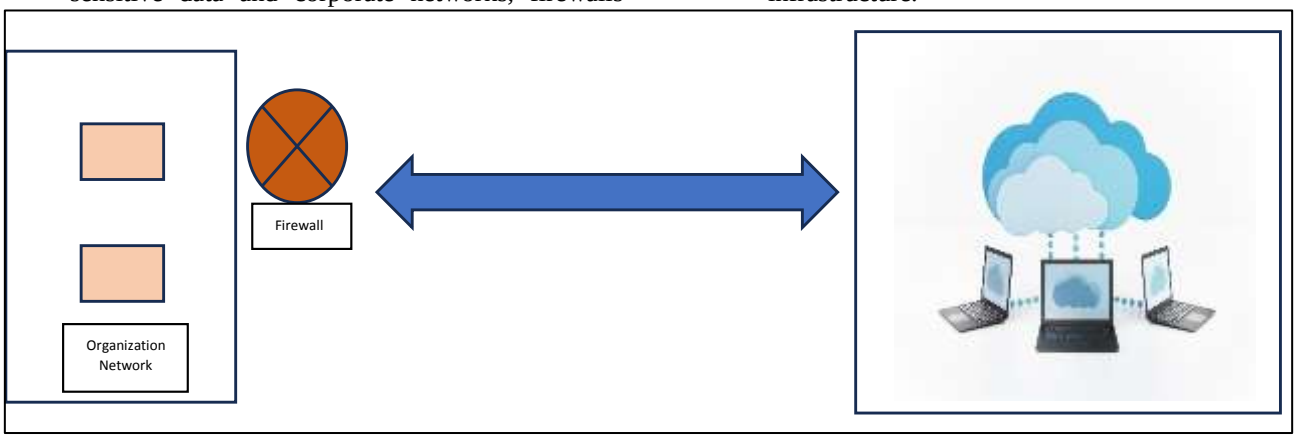


Fig. 12: Firewall

c) Encryption Tools[10], [11], [55]: Encryption tools use cryptographic algorithms to convert data into an unreadable format, which can only be decrypted with the appropriate encryption key. It provides confidentiality and protects sensitive information from unauthorized access.

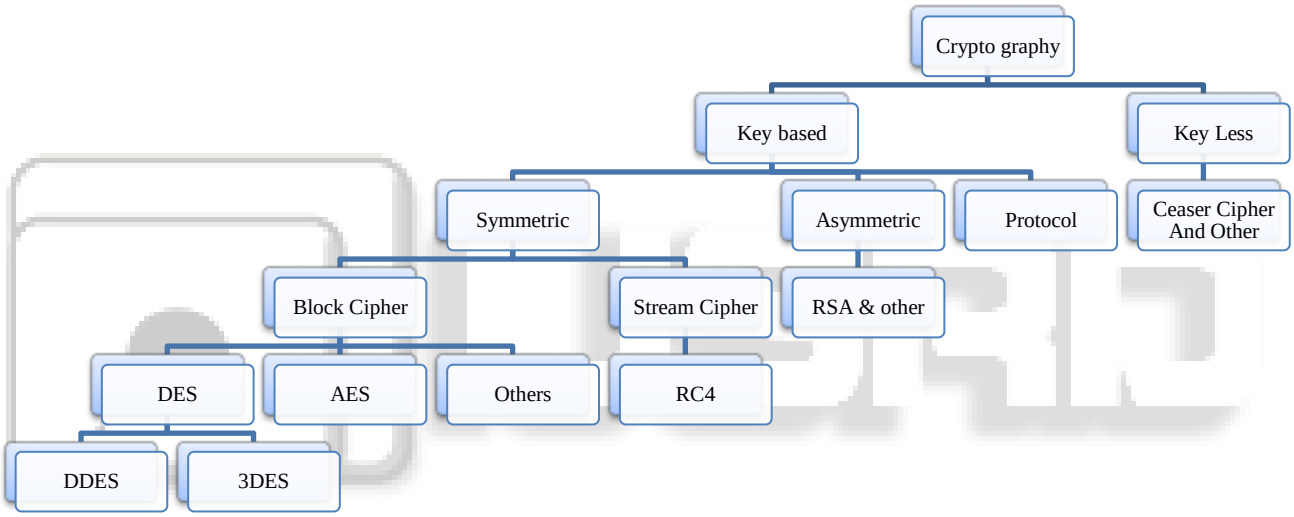


Fig. 13: Overview of cryptographic algorithms

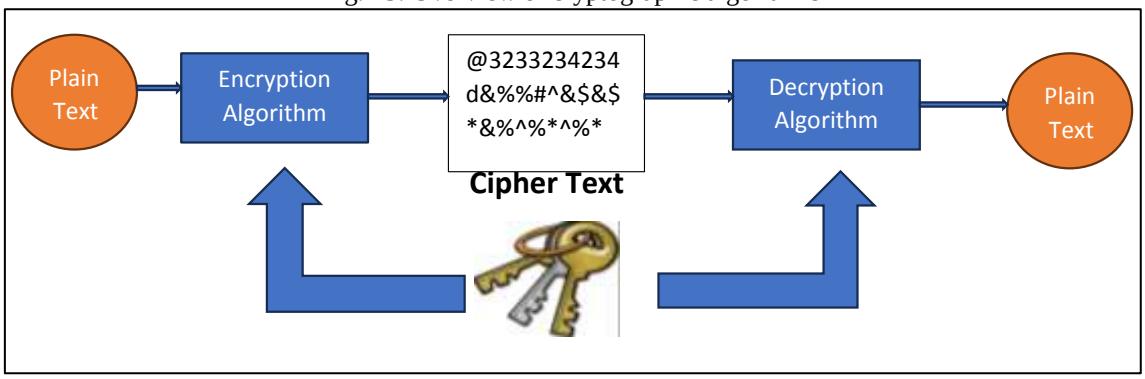


Fig. 14: Overview of Symmetric Cryptography

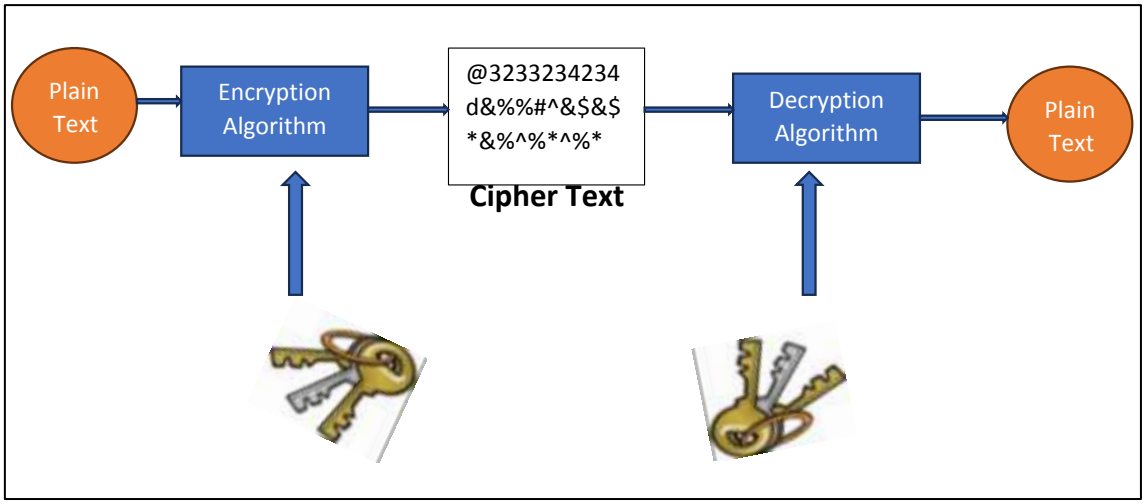


Fig. 15: Overview of Asymmetric Cryptography

d) Penetration Testing Tools[6]: These are tools that simulate cyber-attacks on an organization's network to identify vulnerabilities and weaknesses. Penetration testing tools can help organizations identify and address security gaps before they are exploited by cybercriminals.

e) Intrusion Detection System[52]: A security technology called an intrusion detection system (IDS) is made to track and examine activities taking place on a computer system or network. Its main objective is to spot and warn against any intrusions or unauthorised actions that can jeopardise the availability, confidentiality, and integrity of data and resources. Different IDSs:

S No	IDS Type	Description
1	Exploit-based IDS	A database of known attack signatures is used. evaluate network/system performance in comparison to these signatures. creates notifications when a match is made. provides minimal false positive rates and reliable detection of known attacks.
2	Anomaly-based IDS	builds a model of typical system/network behaviour to provide a baseline of normal behaviour. detects variations from the predetermined baseline. able to recognise unidentified attacks. able to change its attack strategies. higher rate of false positives.

Table 19: Types of Intrusion Detection System

1) Techniques Used in IDS:
   a) Intrusion Detection System (IDS) is a critical area of research in information security and artificial intelligence[52].
   b) IDS is used to identify unauthorized and malicious attacks on computer systems and networks[52].
   c) IDS has two types: misuse-based and anomaly-based[52].
   d) Misuse-based IDS relies on predefined signatures or patterns of known attacks to detect malicious activity[52].
   e) Anomaly-based IDS establishes a baseline of normal behaviour and detects any deviations from this baseline, indicating a potential intrusion[52].
   f) Data mining techniques are widely used in IDS for intrusion detection[52].
   g) These techniques analyse network activities, identify patterns, and classify them as normal or abnormal[52].
   h) Common data mining algorithms used in IDS include Random Forest, Support Vector Machine, Artificial Neural Networks, and C4.5 decision trees[52].
   i) The primary goal of IDS is to protect data from fraudulent users and prevent unauthorized access to computer systems and networks[52].
   j) IDS can detect various types of attacks, such as denial of service (DoS) attacks, filtering attacks (eavesdropping), and access attacks (phishing)[52].
   k) When an IDS detects a security threat, it generates an alert to indicate the presence of an intrusion[52].
   l) Researchers continue to explore and refine data mining techniques to improve the accuracy and effectiveness of IDS[52].
   m) Factors such as the size of the training data set can impact the performance of data mining techniques in IDS[52].
   n) Ongoing research aims to enhance IDS capabilities and address the evolving challenges posed by intrusion attempts[52].

f) Virtual Private Network[53], [54]: A virtual private network (VPN) frequently makes use of a public network, such as the Internet, to link remote locations or users. It establishes secure "tunnels" for data transfer across the open Internet by the encryption of all communication. The network is

shielded from unauthorised users and data eavesdropping by doing this.

g) One component of a VPN is a VPN server, which permits remote access to the company's network and accepts VPN connections from clients. The VPN client establishes the initial connection to the VPN server. There are two different types of VPN connections: router-to-router VPN connections, which connect two different routers in a network, and remote access VPN connections, which allow lone users to connect to a private network.

h) Through internet-based VPN connections, remote access customers can join the company's VPN server. This makes everything affordable and accessible. Typically, the transit inter-network for VPN connections is the Internet or a private IP-based intranet.

i) VPN employs tunnelling technology to control tunnels and encapsulate sensitive information. For instance, Windows 2000 supports the PPTP and L2TP tunnelling protocols. When using a VPN, data is encrypted and wrapped to provide secure transmission over an open TCP/IP network.

j) The suggested method aims to increase security by providing administrators and users with a safe means of exchanging confidential information. Online project assignment distribution is made possible by its admin and client modules, speeding up internal processes. Users can log in to view confidential data on the system's password-protected login page.

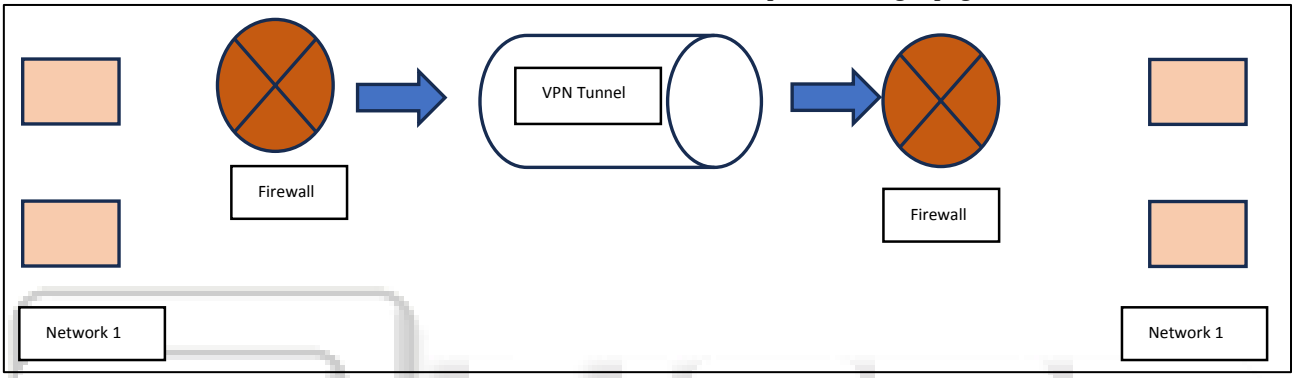


Fig. 16: VPN

k) Secure data transmission, lower expenses owing to the elimination of long-distance charges, and the ability to include branch offices and remote employees into a centralised network are just a few of the ways that VPN may help businesses. An operational, financial, and technological feasibility analysis is crucial during the preliminary research stage of building a VPN system.

l) IPsec[10]: A protocol suite called IPsec (Internet Protocol Security) was created to offer security at the Internet layer (IP layer) of the TCP/IP protocol stack. It secures the data transmitted over IP networks by providing IP packets with authentication, integrity, and confidentiality. IPsec fixes the flaws in IP packets, which are sent in plain text and are susceptible to being intercepted, read, and altered by malevolent parties. Authentication Header (AH) and Encapsulating Security Payload (ESP) are the two primary protocols that make up IPsec. To offer security services, these protocols append additional headers to IP packets.

S No	Protocol	Description
1	Authentication Header (AH)	Provides IP packets with authentication, integrity, and optional anti-replay protection. To secure the integrity of the packet, it adds a header with a cryptographic checksum between the IP header and the contents of the packet. operates in both tunnel and transit modes.
2	Encapsulating Security Payload (ESP)	Offers data secrecy by encrypting the payload of an IP packet. It has optional anti-replay security and authentication. operates in both tunnel and transit modes. before authentication, the packet is encrypted.

Table 20: IP Sec Protocol

The Internet Key Exchange (IKE) protocol is used for key management in IPSec-enabled secure communication. The Security Association (SA), which comprises details on the IPSec protocol version, mode of operation, cryptographic methods, keys, and other characteristics, is created by IKE through negotiations between communicating parties. IPSec has the following uses and benefits:

1) Secure remote internet access: Allows secure connections to an organization's network from remote locations like homes or hotels.
2) Secure branch office connectivity: Enables secure connections between branches of an organization over the Internet instead of expensive leased lines.
3) Interconnectivity between organizations: Facilitates secure and cost-effective connections between the networks of different organizations.

Transparency to end users, compatibility with firewalls, no modifications needed to upper layers (application and transport), protection for all incoming and

outgoing traffic, secure access for staff members who travel, and reasonably priced interconnection between branches and offices are all benefits of IPSec. IPSec is a complex protocol suite, thus it's crucial to keep in mind that its implementation calls for careful configuration and maintenance of security policies, key exchanges, and security associations.

m) TLS/SSL(Ensuring Secure Communication and Data Protection)[51]: Secure communication channels across computer networks are made using the cryptographic protocols Secure Sockets Layer (SSL), which it supersedes, and Transport Layer Security (TLS). TLS/SSL protocols are required to guarantee data integrity, secrecy, and authentication between clients and servers. Through a sequence of handshakes between the client and server, TLS/SSL establishes security. Both sides bargain over the encryption techniques and trade digital certificates to establish identity during this procedure. As a result, data can be transmitted securely, guarding against hacking and unauthorised access. The Record Protocol, Handshake Protocol, Change Cypher Spec Protocol, and Alert Protocol are only a few of the layers that make up the TLS/SSL protocol suite. While the Handshake Protocol handles cryptographic parameter negotiation and authentication, the Record Protocol encrypts application data. The Alert Protocol manages problem and warning warnings, while the Change Cypher Spec Protocol indicates the transition to freshly defined encryption parameters.

TLS/SSL provides a number of cypher suites and encryption techniques, enabling parties to select the right level of security. The management of certificates makes use of public key infrastructure (PKI), which protects the validity and integrity of digital certificates.

TLS/SSL is essential in today's digital environment for safeguarding sensitive data during online transactions. Data including login credentials, financial transactions, and personal information are protected from eavesdropping and unauthorised access. The widespread use of TLS/SSL has greatly improved online security and increased user confidence in online services. A crucial element of network security is TLS/SSL. It has become an essential protocol for data protection due to its capacity to create secure communication channels, use powerful encryption techniques, and validate identities using digital certificates.

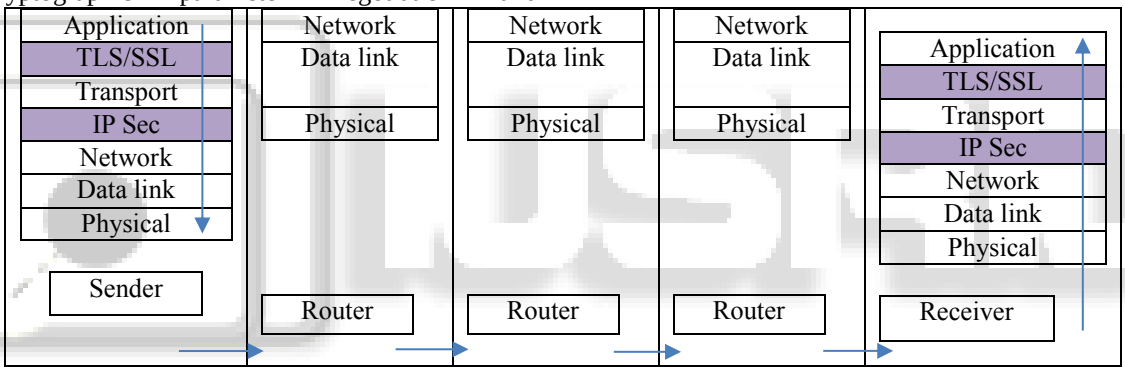


Fig. 21: OSI Security layer

K. Network vulnerability scanning tool:

The actions to perform while assessing a system for vulnerabilities are known as the six Ps: Patch, Ports, Protect, Policies, Probe, and Physical. The fundamental principle of computer security is patch checking. In addition, open ports need to be verified, typical attacks must be avoided, policies need to be reviewed, vulnerabilities need to be investigated, and physical security has to be assessed.[12].

Step	Explanation
Patch[12]	Checking and installing software patches and updates to address known vulnerabilities.
Ports[12]	Verifying open ports on a system, ensuring only necessary ports are open and properly secured.
Protect[12]	Defending against common attacks like malware, phishing, and social engineering.
Policies[12]	Reviewing and updating security policies to ensure they are current and effective.
Probe[12]	Actively probing a system for vulnerabilities using tools like vulnerability scanners and penetration testing.
Physical[12]	Assessing physical security measures, including access controls and surveillance effectiveness.

Table 21: six Ps: Patch, Ports, Protect, Policies, Probe, and Physical

Specific tool to secure Network: The specific tools used will depend on the needs and resources of the organization.

Sr No	Tool	Description
1	MBSA [12]	Microsoft Baseline Security Analyzer (MBSA) is a free tool to scan Windows-based systems for security issues.
2	Nessus[12]	Nessus is a widely-used, commercial vulnerability scanner that identifies network vulnerabilities and misconfigurations.
3	OWASP Zap[12]	OWASP Zap is a free tool for detecting vulnerabilities in web applications, including SQL injection and XSS.

4	Shodan [12]	Shodan is a search engine identifying vulnerabilities in internet-connected devices, aiding in exploit detection.

Table 22: Specific Network Scanning tool

L. Programming Language Specific Cyber Security Software Tool/Library[56]–[61]:

There are several programming language-specific cybersecurity software tools available, designed to address specific security challenges and vulnerabilities. Here are a few examples:

S No	Tool Name	Programming Language	Description
1	CyberSecTK[58], [60]	Python	an easy-to-use Python programme for preprocessing and feature extraction from data related to cyber security. It aims to support data management strategies for cyber security professionals.
2	Scapy[58]	Python	network discovery, packet creation, and network scanning are all made possible via a packet manipulation library. It is often used for network analysis and developing unique network protocols.
3	PyCrypto[58]	Python	Key management, hashing, digital signatures, encryption, and other cryptographic techniques are all provided by a Python module. It is used for secure chat as well as for the sharing of private, confidential data.
4	Metasploit Framework[58]	Python	A Python API-based penetration testing toolkit. Users can automate the processes of exploitation, post-exploitation, and vulnerability evaluation.
5	OWASP ZAP (Python)[58]	Python	a free programme for running penetration tests and evaluating the security of web applications. Programmes written in Python can be used to personalise it.
6	ESLint (JavaScript[57])	JavaScript	a popular JavaScript linter that assists in finding potential security flaws in JavaScript code. It can identify issues like improper API usage and XSS vulnerabilities.
7	FindBugs (Java)[56]	Java	a static analysis tool that finds potential bugs in Java code. It can identify issues like concurrency problems, resource leaks, and null pointer dereferences by examining at the bytecode.
8	PMD (Java)[56]	Java	a Java static analysis tool that places an emphasis on the elegance and excellence of the code. It can identify problems like unnecessary variables, ineffective code, and coding style violations. For the study and improvement of Java code, it provides rules that can be adjusted.
9	JLint (Java)[56]	Java	a simple tool for static analysis of Java programmes. It draws attention to possible weaknesses and frequent programming errors including meaningless variables, dubious expressions, and probably null pointer exceptions.
10	ESC/Java2[56]	Java	a tool for static analysis of Java programmes that uses enhanced static checking. Formal verification approaches are used to identify potential programming flaws such as null dereferences, array bounds violations, and concurrency issues.

Table 23: Programming Language Specific Cyber Security Software Tool

III. Conclusion:

The examination of cybersecurity patterns, challenges, and solutions presented in this study paper reveals critical conclusions that demand careful consideration. The findings underscore the complexity and urgency of the cybersecurity landscape, emphasizing the necessity of proactive action to combat emerging threats effectively.

Firstly, the study highlights the alarming increase in cyber-attacks and data breaches due to the world's growing dependence on the internet. This underscores the importance of equipping individuals and organizations with the knowledge and skills required to recognize and prevent cyber-attacks, with a particular focus on comprehensive staff training programs.

Secondly, learning from past mistakes and adopting preventive measures is crucial to safeguard digital assets. Failure to do so can lead to recurrent cyber-attacks, posing severe threats to both individuals and corporations. Continual development of cybersecurity strategies and staying abreast of evolving threats are imperative for organizations.

Thirdly, the prevalence of cyber risks, such as phishing schemes, ransomware, and identity theft, emphasizes the need for heightened awareness and robust preventive measures. Vigilance, strong security protocols, and staying informed about current cyber threats are essential for personal and organizational security.

The research also sheds light on the vulnerability of small enterprises due to the handling of personally identifiable information. Recognizing this vulnerability, small businesses must invest in cybersecurity measures and adhere to best practices to protect client data effectively.

The imperative for stronger cybersecurity measures is further underscored by predictions of exponential data storage growth and rising global costs of cybercrime. Prioritizing data protection, implementing stringent security procedures, and utilizing cutting-edge technologies are essential for preserving critical information.

Additionally, the underreporting of cybercrimes hampers efforts to fully comprehend the scope and consequences of cyber-attacks. Encouraging reporting channels and creating a supportive environment that respects victims' privacy and reputation are necessary to address this issue and enable more accurate analysis of cybercrime trends.

The case study of the roles played by specialized agencies, such as the IC3 and the FBI, in combating cybercrime emphasizes their vital efforts in addressing concerns, educating the public, and publishing intelligence reports. Collaborative initiatives between authorities, corporations, and individuals are crucial for effectively countering persistent and dynamic cyber threats, ranging from DDoS assaults to phishing schemes and cyber espionage.

The research underscores the critical significance of cybersecurity in today's interconnected world. Implementing proactive measures, raising awareness, encouraging international cooperation, and addressing the cybersecurity talent gap are vital to improving global defences and mitigating the risks posed by cybercrime. By taking a multifaceted approach and prioritizing cybersecurity, we can create a safer online environment for people, businesses, and governments worldwide.

The security measures outlined in this study paper offer organizations the means to substantially enhance their security posture, fortifying them against potential threats. Embracing protocol-level security measures, leveraging cryptographic mechanisms, IDS, firewalls, and VPNs, and adopting a proactive defence approach all contribute to establishing a resilient and invulnerable security framework. With a comprehensive and agile defence strategy in place, organizations can confidently safeguard their critical assets, protect against data breaches, and ensure sustained business continuity amidst the ever-evolving landscape of cyber threats.

REFERENCES:

[1] Steve Morgan Editor-in-Chief, "2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics," Cybersecurity Ventures, Jan. 19, 2022.
[2] Steve Morgan Editor-in-Chief at Cybersecurity Ventures, "Cybercrime Infographics: Illustrations Of The Past, Present, And Future Threats We Face," Cybersecurity Ventures, Mar. 24, 2020. https://cybersecurityventures.com/cybercrime-infographic/ (accessed Apr. 22, 2023).
[3] Paul Abbate Deputy Director Federal Bureau of Investigation, "Federal Bureau of Investigation Internet Crime Report 2021," US, 2022. Accessed: Apr. 24, 2023. [Online]. Available: https://www.ic3.gov/
[4] Timothy Langan Executive Assistant Director Federal Bureau of Investigation, "Federal Bureau of Investigation Internet Crime Report 2022," US, 2023. Accessed: Apr. 24, 2023. [Online]. Available: https://www.ic3.gov/
[5] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and Their Classification," 2013.
[6] Dr. Y. Perwej, S. Qamar Abbas, J. Pratap Dixit, Dr. N. Akhtar, and A. Kumar Jaiswal, "A Systematic Literature Review on the Cyber Security," International Journal of Scientific Research and Management, vol. 9, no. 12, pp. 669–710, Dec. 2021, doi: 10.18535/ijsrm/v9i12.ec04.
[7] Center for Strategic and International Studies, "Significant Cyber Incidents (CSIS)," Significant Cyber Incidents (CSIS), 2023, Accessed: Apr. 26, 2023. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[8] S. P. M. F. S. B. Alexis M Pitney, "A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities," IEEE, vol. 1, no. 1, pp. 1–1, Aug. 2022.
[9] Dr. S. C. B. Lamar, M. Kuralt, and C. Zidor-Guerrier, "Enterprise Risk Management Post Solar Winds Hack," International Journal of Business and Applied Social Science, pp. 13–19, Sep. 2021, doi: 10.33642/ijbass.v7n9p2.
[10] Atul Kahate, "Cryptography and Network Security Third Edition."
[11] Behrouz Forouzan, "Cryptography Network Security (Behrouz Forouzan)".
[12] Chuck Easttom, "Computer Security Fundamentals, Fourth Edition (Chuck Easttom)," Pearson.
[13] wikipedia, "McCumber cube," Assessing and Managing Security Risk in IT Systems: A Structured Methodology, 2023. https://en.wikipedia.org/wiki/McCumber_cube (accessed Aug. 05, 2023).
[14] POA Publishing., Asset protection and security management handbook. Auerbach Publications, 2003.
[15] EUROPOL, "Cybercrime," EUROPOL. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime (accessed Jul. 04, 2023).
[16] J. Singh, S. Kaur, G. Kaur, and G. Kaur, "A Detailed Survey and Classification of Commonly Recurring Cyber Attacks," 2016.
[17] V. Papaspirou, L. Maglaras, and M. A. Ferrag, "A tutorial on Cross Site Scripting Attack - Defense," 2020, doi: 10.3390/computersxx010005.
[18] B. K. Ayeni, J. B. Sahalu, and K. R. Adeyanju, "Detecting Cross-Site Scripting in Web Applications Using Fuzzy Inference System," Journal of Computer

Networks and Communications, vol. 2018, 2018, doi: 10.1155/2018/8159548.
[19] J. M. Howe and F. A. Mereani, "Detecting Cross-Site Scripting Attacks Using Machine Learning," vol. 723, 2018, doi: 10.1007/978.
[20] A. W. Marashdih and Z. F. Zaaba, "Cross Site Scripting: Detection Approaches in Web Application," 2016. [Online]. Available: www.ijacsa.thesai.org
[21] V. Abdullayev and Dr. A. S. Chauhan, "SQL Injection Attack: Quick View," Mesopotamian Journal of Cyber Security, pp. 30–34, Feb. 2023, doi: 10.58496/mjcs/2023/006.
[22] Y. S. Jang, "Detection of SQL injection vulnerability in embedded SQL," IEICE Trans Inf Syst, vol. E103D, no. 5, pp. 1173–1176, May 2020, doi: 10.1587/transinf.2019EDL8143.
[23] D. Chen, Q. Yan, C. Wu, and J. Zhao, "SQL Injection Attack Detection and Prevention Techniques Using Deep Learning," in Journal of Physics: Conference Series, IOP Publishing Ltd, Feb. 2021. doi: 10.1088/1742-6596/1757/1/012055.
[24] M. Alghawazi, D. Alghazzawi, and S. Alarifi, "Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review," Journal of Cybersecurity and Privacy, vol. 2, no. 4, pp. 764–777, Sep. 2022, doi: 10.3390/jcp2040039.
[25] G. Shrivastava and K. Pathak, "SQL Injection Attacks: Technique and Prevention Mechanism," 2013.
[26] F. Q. Kareem et al., "SQL Injection Attacks Prevention System Technology: Review," Asian Journal of Research in Computer Science, pp. 13–32, Jul. 2021, doi: 10.9734/ajrcos/2021/v10i330242.
[27] A. Kie, zun Mit, P. J. Guo, K. Jayaraman, and M. D. Ernst, "Automatic Creation of SQL Injection and Cross-Site Scripting Attacks." [Online]. Available: http://www.mysite.com/?mode=display&topicid=1
[28] J. Erasmus, "Anatomy of a malware attack," Network Security, vol. 2009, no. 1, pp. 4–7, Jan. 2009, doi: 10.1016/S1353-4858(09)70005-4.
[29] E. Gandotra, D. Bansal, and S. Sofat, "Malware Analysis and Classification: A Survey," Journal of Information Security, vol. 05, no. 02, pp. 56–64, 2014, doi: 10.4236/jis.2014.52006.
[30] N. Khairani Kamarudin, N. Nazifabinti Md Hasani, R. Ruslan, N. Hidayah Ahmad Zukri, and I. Hazwam Abd Halim, "The Performance Analysis Of Malware Attack," 2018.
[31] IEEE Staff and IEEE Staff, A Survey of Phishing Attack Techniques. 2014.
[32] D. Patel, "All about Phishing Attack, Danger and Its Prevention," Int J Res Appl Sci Eng Technol, vol. 10, no. 6, pp. 4908–4914, Jun. 2022, doi: 10.22214/ijraset.2022.45109.
[33] Amit Kumar, "Cyber Security Issues and Challenges - A Review," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, pp. 269–273, Jun. 2022, doi: 10.32628/cseit228379.
[34] S. Khurana, "A Review Paper on Cyber Security," 2017. [Online]. Available: https://en.wikipedia.org/wiki/Malware
[35] K. Y. Chai and M. F. Zolkipli, "Review on Confidentiality, Integrity and Availability in Information Security," Journal of ICT In Education, vol. 8, no. 2, pp. 34–42, Jul. 2021, doi: 10.37134/jictie.vol8.2.4.2021.
[36] Shruti Sunil Ajankar and Aditi Rajesh Nimodiya, "Cyber Security : Techniques and Perspectives on Transforming - A Review," Int J Sci Res Sci Technol, pp. 473–480, Dec. 2021, doi: 10.32628/ijsrst218670.
[37] A. Bonguet and M. Bellaiche, "A survey of Denial-of-Service and distributed Denial of Service attacks and defenses in cloud computing," Future Internet, vol. 9, no. 3, Aug. 2017, doi: 10.3390/fi9030043.
[38] V. Sharma et al., CRITICAL INVESTIGATION OF DENIAL OFSERVICE AND DISTRIBUTED DENIAL OF SERVICEMODELS AND TOOLS. 2018.
[39] A. 2016 nternational Journal of Computer Applications (0975 –8887)Volume 139 –No.1, "A Review on Phishing Attacks and Various Anti Phishing Techniques," 2016.
[40] A. Shankar, R. Shetty, and B. Nath, "A Review on Phishing Attacks," 2019. [Online]. Available: http://www.ripublication.com
[41] Y. Tiwari and M. Tiwari, "A Study of SQL of Injections Techniques and their Prevention Methods," 2015. [Online]. Available: www.ijcaonline.org
[42] Z. Habibi, "A review on the comparable analyses of SQL injection: attacks, vulnerabilities, and their detection techniques," ~ 6 ~ International Journal of Advanced Academic Studies, vol. 2, no. 1, 2020, [Online]. Available: http://www.toolsmarket-
[43] J. P. Singh, "Analysis of SQL Injection Detection Techniques." [Online]. Available: http://exploitable-web.com/link.php?id=1'
[44] H. Shahriar, S. North, and W.-C. Chen, "Early Detection of SQL Injection Attacks," International Journal of Network Security & Its Applications, vol. 5, no. 4, pp. 53–65, Jul. 2013, doi: 10.5121/ijnsa.2013.5404.
[45] R. Rawat and S. K. Shrivastav, "SQL injection attack Detection using SVM," 2012.
[46] B. Shehu and A. Xhuvani, "A Literature Review and Comparative Analyses on SQL Injection: Vulnerabilities, Attacks and their Prevention and Detection Techniques," 2014. [Online]. Available: www.IJCSI.org
[47] K. Baptista, A. Bernardino, and E. Bernardino, EXPLORING SQL INJECTION VULNERABILITIES USING ARTIFICIAL BEE COLONY. 2021.
[48] Z. Chen, M. Guo, and L. Zhou, "Research on SQL injection detection technology based on SVM," MATEC Web of Conferences 173, (2018), 2018, doi: 10.1051/matecconf/2018173.
[49] K. Ahmad and M. Karim, "A Method to Prevent SQL Injection Attack using an Improved Parameterized Stored Procedure." [Online]. Available: www.ijacsa.thesai.org
[50] A. Alzahrani, A. Alqazzaz, N. Almashfi, H. Fu, and Y. Zhu, "Web Application Security Tools Analysis," Stud Media Commun, vol. 5, no. 2, p. 118, Nov. 2017, doi: 10.11114/smc.v5i2.2663.
[51] A. Satapathy and J. Livingston, "A Comprehensive Survey on SSL/ TLS and their Vulnerabilities," 2016.

[52] C. Kiran Kumar and M. Govindarajan, "Intrusion Detection System Using Data Mining Techniques-A Survey," International Journal of Research in Advent Technology, vol. 7, no. 4, 2019, [Online]. Available: www.ijrat.org
[53] P. MEHTA, "Security of Virtual Private Network," Journal of University of Shanghai for Science and Technology, vol. 23, no. 3, Mar. 2021, doi: 10.51201/jusst12647.
[54] A. Sikora and P. Brügger, "Virtual Private Infrastructure (VPI) Initiative-An Industry Consortium for Unified and Secure Web Control with Embedded Devices."
[55] M. F. Mushtaq et al., "A Survey on the Cryptographic Encryption Algorithms," 2017. [Online]. Available: www.ijacsa.thesai.org
[56] N. Rutar, C. B. Almazan, and J. S. Foster, "A Comparison of Bug Finding Tools for Java *."
[57] K. Fjóla Tómasdóttir, "Why and How JavaScript Developers Use Linters." [Online]. Available: www.ewi.tudelft.nl
[58] J. Seitz, T. Arnold, and an O. M. Company. Safari, Black Hat Python, 2nd Edition.
[59] K. Erickson, "Hacker Basic Security Learning Effective Methods of Security and How to Manage Cyber Risks Awareness Program with Attack and Defense Strategy Tools Art of Exploitation in Hacking," 2019.
[60] R. A. Calix, S. B. Singh, T. Chen, D. Zhang, and M. Tu, "Cyber security tool kit (cybersectk): A python library for machine learning and cyber security," Information (Switzerland), vol. 11, no. 2, Feb. 2020, doi: 10.3390/info11020100.
[61] R. A. Calix, S. B. Singh, T. Chen, D. Zhang, and M. Tu, "Cyber security tool kit (cybersectk): A python library for machine learning and cyber security," Information (Switzerland), vol. 11, no. 2, Feb. 2020, doi: 10.3390/info11020100.

