ADVANCE CYBER ATTACKS

# ABSTRACT

The threat of cyber attacks is a serious one in today's world where global economic, business, cultural, sociocultural, and political activities are mostly done on the Internet. Many private corporations and governmental bodies around the world have increased their vulnerability to sophisticated cyber-attacks because of the expansion in wireless communication technologies. The preservation of data from these techniques has become a highly intricate emergency issue given society’s overreliance on electrical technology.

In reality, cyber-attacks are not just a bother but are always planned to harm firms financially. In addition to financial losses, these attacks may have military or political objectives as well. Organizations of all sizes face extensive risks from different types of cyber threats like personal computer viruses, data breaches, and distributed denial-of-service (DDoS) attacks. Therefore, organizations utilize several measures to minimize the impacts of cyber-attacks including real-time information and use of advanced technologies aimed at strengthening their security.

To confront new cyber threats, researchers all over the world have recommended numerous techniques for preventing cyber attacks and reducing their effects. These methods embrace operational solutions that are currently in use as well as those under study and development. This research intends to individually examine the improvements in cybersecurity by looking at their efficiency as well as assessing weaknesses, challenges, and strengths associated with each approach.

Furthermore, this research explores advanced cyber attacks from their different aspects i.e. a new descendant attack vector is described in detail. The paper also traces the history of standard security frameworks and discusses early-generation cyber security methodologies. Additionally, it looks at the emerging trends and recent developments within the field highlighting new security threats and challenges they present.

This study aims to offer valuable insights for IT professionals and cyber security researchers by presenting a thorough review of the latest advances in cyber security. It is hoped that this comprehensive investigation will be a useful information source for future research and be important in formulating strategies effective in fighting cyber threats in a more and more digital world.

# INTRODUCTION

A **Cyber Attack** is an attack in which a person aims at stealing, disabling, destroying information, or gaining access to one’s software. Every day people become victims of cyber-attacks in many ways like mobile malware, logging in to illegal websites, opening random links, downloading any app without having any antivirus software etc.

Many steps have been taken to reduce cyber attacks by keeping your steps configured, installing a firewall, keeping a backup, keeping a strong password, and updating your antivirus software.

An **advanced cyber attack** is an attack where a hacker has authorized power over your network and it remains unidentified. There are many advanced cyber attacks like – DoS DDoS attacks, MITM attacks, Phishing attacks, etc.

There are different stages of an advanced cyber attack – reconnaissance, weaponization, delivery, exploitation, installation, command, and control.



To avoid cyber attacks every company keeps its systems and devices updated and configured:

* An antivirus is software that protects the computer if it detects any threats it takes action to clear them. it uses a database of knowledge to identify and block malicious and suspicious programs it is the bodyguard of your system.
* A firewall acts as a cover between your device and the internet. It uses a set of rules and decides whether to block or allow the signals , by this process the firewall helps in unauthorized access to your computer , it behaves like a security guard .
* Vulnerability management rules consisting of patch management and regular penetration testing can help catch and stop cyber attacks. It is a type of unethical hacking .
* Attack surface management: tools that can identify, catalog, and remediate potentially vulnerable assets define instances of risks before cyberattackers will locate them first attack.
* UEM tools: They can enforce security policies and controls over all endpoints on the corporate network, which include laptops, desktops, and mobile phones.
* Security awareness training: training modules that can help users understand and avoid some of the most typical cyberattacks

Cyber attacks can damage and destroy and cause a lot of loss to an organization and business. The average cost of breached data is 43.5 million. Cyber attacks happen for criminal, political, and personal reasons . The cyber attack targets include money, business data, client lists, email addresses personal credentials etc .

If effective, cyberattacks can damage ventures. They can create downtime, information loss as well as cash loss. As an example:

Cyberpunks can make use of malware or denial-of-service strikes to create system or web server collisions. This downtime can cause significant solution disturbances as well as economic losses. According to the Cost of a Data Breach record the typical violation caused USD 1.42 million in shed service. SQL shot strikes enable cyberpunks to modify, erase, or take information from a system. Phishing assaults permit cyberpunks to deceive individuals right into sending out cash or delicate details to them. Ransomware strikes can disable a system up until the business pays the assailant ransom money. According to one record (web link lives beyond ibm.com) the ordinary ransom money repayment is USD 812,360.

In addition to directly damaging the target, cyberattacks can have a host of second prices and also repercussions. For instance the Expense of an Information Violation record discovered that services invest approximately USD 2.62 million on spotting, reacting to, as well as relieving violations. Cyberattacks can additionally have effects on sufferers past the prompt target. In 2021, the DarkSide ransomware gang struck the Colonial Pipe, the biggest fine-tuned oil pipe system in the United States. The opponents got into the business's network by utilizing a jeopardized password (the web link lives outside ibm.com). They stopped the pipe that lugs 45% of the gas, diesel, and also jet gas provided to the United States East Coast, resulting in extensive gas. The cybercriminals required ransom money of nearly USD 5 million in bitcoin cryptocurrency, which Colonial Pipe paid (web link lives outside ibm.com). Nonetheless, with aid from the United States federal government, the firm at some point recuperated USD 2.3 million of the ransom.

# LITERATURE REVIEW

"Understanding along with being prepared is the initial line of defense versus cyber hazards as well as cybercrimes, e.g. by details safety and security training. Educating can take 2 kinds the very first is focused on protection experts as well as intends to boost comprehending of the current hazards as well as to raise ability degrees in protecting together with minimizing versus them. The purpose of this paper is to look into the suggestion of a cyber array, as well as to consist of a thorough evaluation of literary works covering unclassified cyber arrays and safety and security examination beds [1] In this evaluation we develop a taxonomy for cyber array systems and also assess existing literary works that concentrate on style coupled with situations yet likewise capabilities features sources and so on In this paper the IoT-based wise grid's threats plus future methods are evaluated as well as concentrate on kinds of cyber hazards as well as consist of a thorough of the clever grid's cyber-security setting. In specific we focus on dealing with along with evaluating susceptibilities in the network, tough actions, and calling for defense. We aim to offer a deep understanding of cyber-security vulnerabilities and options as well as offer a plan for future cyber-security study instructions in clever grid applications [2].

A cyber safety and security control V&V procedure version is improved in this research study to address the issue based on the concept of flexible concentrating screening. In addition, a measurable method is constructed to specify and also focus on fault-prone details safety and security controls. It has been confirmed that the design developed might give an extra and also a lot more reputable structure for specialists very subjective judgment [3] This short article concentrates on the value of various cyber protection requirements, plus cyber safety and security structure style. We talk about protection dangers, attacks, and also cyber safety steps. After that, we review the various problems of standardization of cyber safety. We likewise attend to the nationwide info safety and security plan to safeguard the online world together with different federal government approaches in safeguarding cyber safety and security. Ultimately we have some essential standards for details safety together with details safety [4] This paper reviews the demands needed for the Federal Government's examination of cybersecurity plans for the United States Department of Health as well as Human Services. The overarching purpose of cybersecurity plans together with treatments is to make it possible by conformity with well-known Federal guidelines and also criteria to shield the functional sources along with objectives of the United States Department of Health and Human Resources and also to motivate ideal methods of safety and security in the protection of info systems versus unapproved stars plus cyber hazards [5] This automation lowers human mistakes in order handling, and also raises order shipment efficiency. Nevertheless strikes from the room, specifically from the Internet, can interrupt that. In this paper, we suggest a unique attacker-defender design versus an opponent of the quantum feedback (QR) to safeguard vital properties by thinking about the protecting spending plan and also the dependence on homes. The security degree of each property in the option shows its good looks to be protected [6] This paper presents a study of deep discovering methods for spotting cyber safety and security strike the datasets utilized as well as a relative evaluation.

Especially we offer an introduction of breach discovery systems concentrated on deep understanding methods. The data source plays a crucial duty in breach discovery so we specify 35 widely known cyber data sources coupled with team such data sources right into 7 groups: network web traffic data source, electrical network data source, net web traffic data source, digital exclusive network data source, android tool data source, IoT web traffic data source, and also net web link [7] Maker knowing strategies are typically made use of in the production of an invasion discovery system (IDS) for the prompt plus automated discovery as well as category of cyberattacks at network as well as host prices. Nonetheless, when harmful strikes are continuously advancing and also happen in large amounts needing a scalable option several troubles show up. There are numerous data sources of malware openly available for more research study by the detail’s safety area [8] The utmost objective of this research is to instantly and effectively discover practical attribute depictions from huge amounts of unlabeled raw network web traffic information by utilizing deep knowing methods. We recommend a unique violation version for the network by piling expanded coevolutionary car encoders and examining our strategy on 2 brand-new data sources for breach discovery. Several types of research have been accomplished to examine whether our technique achieves success [9] This paper creates the discovery engine with numerous innovative deep-knowing versions and executes a measurable as well as relative analysis of these versions we study the usefulness of off-line deep understanding-based NIDSes. Initially, we provide the basic method of deep understanding as well as its academic repercussions for the concern of network breach discovery. After that assess numerous devices discovering services for 2 jobs of network invasion discovery [10]".

# CYBERCRIME OVERVIEW

Cyber attacks globally increased by 125% in 2021 compared to 2020, and increasing volumes of cyber attacks continued to threaten businesses and individuals in 2022.

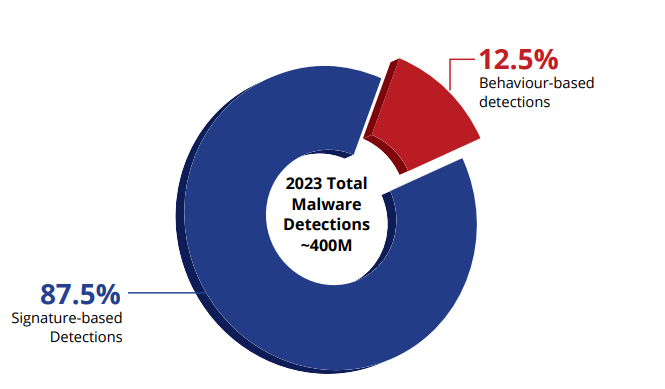
The average cost of data breaches per hour worldwide has also increased. In 2001, the average cost per hour to individuals was $2054. Since then, the hourly loss rate has increased, standing in 2021 at $787,671.

Poland has the strongest cyber security, according to the National Cyber Security Index.

The NCSI measures a country’s ability to prevent cyber threats and manage cyber incidents. As of December 2023, the 5 countries with the highest scores on the NCSI are:

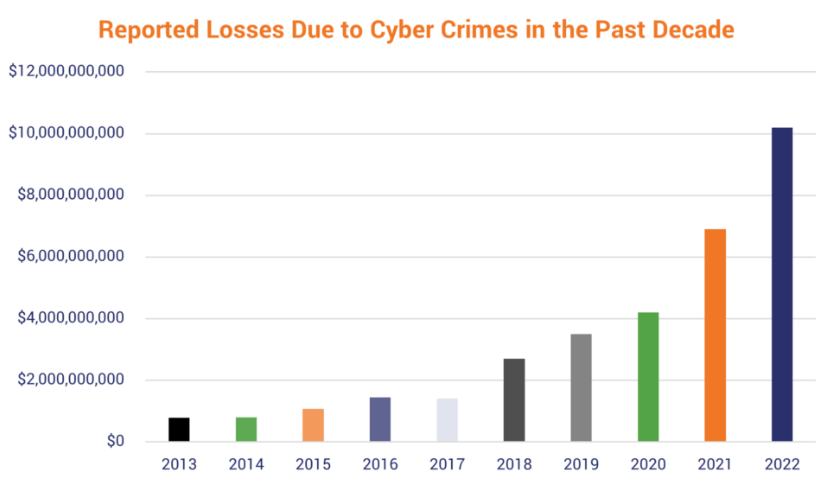
* Poland (90.83)
* Estonia (85.83)
* Ukraine (80.83)
* Latvia (79.17)
* United Kingdom (75.00)

To arrive at the cyber threat landscape of India for the year 2023, a substantial 400 million instances of malware were observed across an extensive network of 8.5 million endpoints. Behavioural Detection (NGAV) played a pivotal role, contributing to 49 million1 of the total detections.

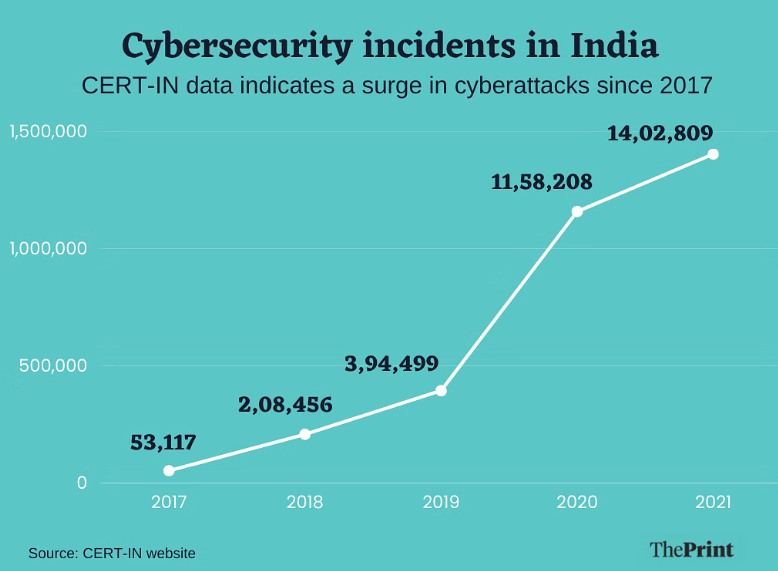


With hacking incidents registering an increase in 2023, nearly two in five (33%) web users in India faced a form of Internet-born cyberattack in 2023, a new report said, highlighting two prominent ways that hackers use to target Indians online.  
According to the global cybersecurity company Kaspersky, a total of 62,574,546 Internet-borne cyber threats were detected and blocked in the country.

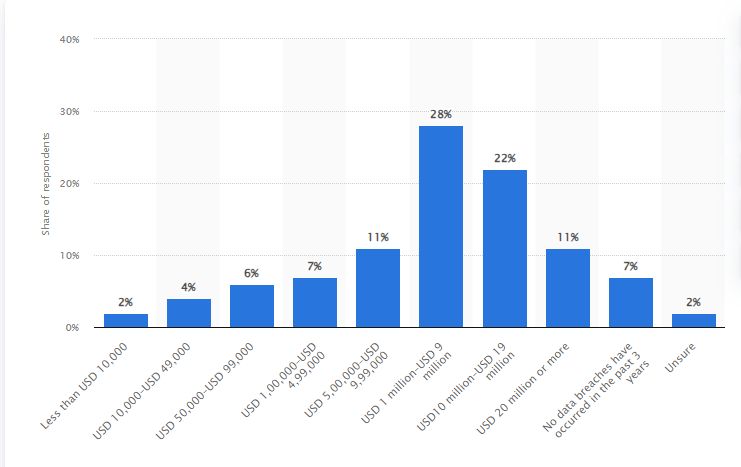
Comparative Charts:



The FBI’s Internet Crime Complaint Center (IC3) reports that although cybercrime reports decreased 5% to 800,944 in 2022, the potential losses from those reported crimes exceeded $10.2 billion for the year. That’s more than double the total losses reported in 2020.



The number of incidents handled by CERT-In surged in 2020 to 11,58,208, a near-tripling over the previous year. This surge continued in 2021, which saw 14,02,809 incidents, a 21 percent increase.



In a 2023 survey on cybersecurity readiness, 28 percent of the surveyed senior business, tech, and security executives in India claimed the damage caused by cyberattacks within their organizations over the past three years was worth between one and nine million U.S. dollars. Meanwhile, only seven percent of respondents attested to not having experienced any data breaches over that period. The rate of cybercrime in India has increased dramatically over the past few years.

# EXISTING CYBER ATTACKS

**JBS Foods Ransomware Attack (2021):**  
JBS Foods, one of the world's largest food companies, suffered a ransomware attack that disrupted its operations in North America and Australia.  
The strike forced JBS to close many restaurants, raising concerns about meat shortages and product disruptions.  
Like the Colonial Pipeline attack, this incident demonstrates the significant impact a ransomware attack can have on critical systems and equipment worldwide.  
Kaseya VSA Supply Chain Ransomware Attack (2021):  
  
Kaseya VSA supply chain attacks target managed service providers (MSPs) that use the widely used Kaseya VSA software platform for monitoring and remote control.  
Attackers exploited a zero-day vulnerability in Kaseya VSA software to distribute ransomware to the networks of Kaseya customers, including hundreds of businesses and organizations.  
The attack led to widespread attacks and data encryption, with attackers demanding a $70 million ransom in Bitcoin for the global decryptor.  
This incident highlights the risks associated with product attacks and the need for the MSP industry to strengthen security measures and oversight.  
These attacks serve as a reminder of the changing threat landscape and the importance of cybersecurity protection, including vulnerability management, primarily threat detection, crisis response planning, and personnel training.

**Microsoft Exchange Server Vulnerabilities (2021):**  
In early 2021, we discovered several zero-day vulnerabilities in native versions of Microsoft Exchange Server.  
Threat actors, including national security groups, use these vulnerabilities to gain unauthorized access to email accounts and configure websites to be accessed regularly.

The attack, first attributed to a proChina group called Hafnium, affected thousands of organizations around the world.  
Microsoft released an emergency patch to fix these issues and called on organizations to apply the patch immediately to reduce the risk of abuse.  
Facebook Data Breach (2018):  
  
In September 2018, Facebook announced a major security breach affecting approximately 50 million user accounts.  
The leak stems from a flaw in Facebook's "Watch As" feature that allows attackers to steal access tokens and bypass a user's account without a password.  
Access tokens can allow an attacker to access a user's personal information, private messages, and other sensitive information.  
Facebook notified affected users, reset their tokens, and implemented additional security measures to prevent similar incidents from occurring in the future.

**WannaCry Ransomware Attack (2017):**  
  
The WannaCry ransomware attack occurred in May 2017 and spread worldwide, infecting hundreds of thousands of computers in more than 150 countries.  
WannaCry exploited a vulnerability in the Microsoft Windows SMB (Server Message Block) protocol called EternalBlue, which was allegedly created by the US National Security Agency (NSA) and then by a group called Shadow Brokers.  
Ransomware encrypts the data of the infected virus demands a ransom in Bitcoins and threatens to permanently delete the data if payment is not made.  
WannaCry affected many organizations, including healthcare organizations, financial services companies, government agencies, and businesses, demonstrating the widespread impact of the outage against ransomware and the importance of domain management.

**Equifax Data Breach (2017)**  
In September 2017, Equifax, one of the largest credit reporting agencies in the United States, disclosed a massive data breach in which the personal information of approximately 147 million customers was leaked.  
The breach occurred due to a flaw in the Apache Struts web application system that Equifax was unable to patch months before the breach.  
An attacker used this vulnerability to gain unauthorized access to Equifax systems and steal many sensitive information, including names, Social Security numbers, dates of birth, addresses and residence information, and credit card information.  
The breach had far-reaching consequences; It resulted in congressional hearings, administrative oversight, numerous lawsuits, and huge damages. Equifax.

**Yahoo data breach (2013-2014, 2016):**  
Yahoo, once a major player in the Internet industry, faced two actions. A serious crime that affects millions of users.  
The breach first reported in 2016 but occurring in 2013, affected more than 1 billion Yahoo accounts, involving the theft of names, email addresses, phone numbers, and hashed passwords.  
The second breach, reported in 2017 but occurring in 2014, affected more than 500 million Yahoo accounts and involved similar data.  
The leak greatly affected Yahoo's reputation and cost the company dearly when it was acquired by Verizon Communications.

**SWIFT Banking System Attacks (2016-2018):**  
SWIFT (Society for Worldwide Interbank Financial Telecommunication) banking system was used to commit fraud in many cyber attacks targeting the financial sector.  
The 2016 Bangladesh Bank Robbery involved the theft of $81 million from Bangladesh Bank's account at the Federal Reserve Bank of New York.  
Similar attacks targeted other banks, international funds using cybersecurity protections and SWIFT messaging capabilities. Transfer the money to the management account.

**Uber Data Breach (2016):**  
In 2016, ride-hailing company Uber suffered a data breach that exposed the personal information of 57 million customers and drivers worldwide.  
The breach occurred when hackers gained permission to access Uber servers and steal sensitive information, including names, email addresses, phone numbers, and driver numbers.  
Rather than immediately report the breach to regulators and implicate individuals, Uber paid hackers $100,000 to remove the stolen data and remain silent about committing the crime.  
The incident sparked outrage and scrutiny from regulators, leading to investigations, lawsuits , and fines against Uber for regulatory violations and blocking user data.  
Marriott International Data Breach (2018):  
In November 2018, Marriott International disclosed a data breach that exposed the personal information of approximately 500 million guests staying at Marriott's Starwood hotels.  
The breach, which began in 2014 but was not discovered until September 2018, involved unauthorized access to Starwood's guest greeting information.  
The stolen information included hotel guests' names, postal addresses, telephone numbers, e-mail addresses, passport numbers, and credit card payment information.  
The case is one of the largest in history, resulting in regulatory scrutiny, litigation, and a significant financial impact on Marriott International.  
These cyber-attacks are a sobering reminder of the ongoing challenges and threats to organizations protecting their systems, networks, and sensitive data from bad people. They emphasized the importance of cybersecurity measures, effective resolution plans, and transparent, communication to reduce risks and reduce the impact of security breaches.

# CONCLUSION

The potential threat, to humanity lies in the escalating cyber chaos that instills fear as it continues to grow until the day when crucial information becomes online. In the study we will explore the advantages and disadvantages of security solutions for types of cyber attacks and their corresponding protective measures. We will delve into the evolution from attack methods to the utilization of Artificial Intelligence, Machine Learning and Genetic algorithms in this field. It is intriguing to ponder whether the sophistication levels being achieved in Cyber Security will surpass all security challenges; however it is concerning that advancements are occurring at a pace, on the dark side of this domain. Moving forward new security innovations will emerge to enhance efficiency and communication capabilities.