Available online at www.qu.edu.iq/journalcm

JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS

ISSN:2521-3504(online) ISSN:2074-0204(print)

Cybersecurity in the Age of the Internet of Things (Threats, Vulnerabilities, Attacks, and Countermeasures): A review

Nada Khaleel Kareem[a] , *Amal Sufiuh Ajrash*[a], *Wildan Jameel Hadi*[a], *Sahar Moneam Salman* [a], *Ammar Hussein Jassim, Raja'a M.Mohammed* [a], *Laith Abualigah* [b]

[a] *Computer Science Department, College of Science for Women, University of Baghdad, Iraq.Email: nada.k@csw.uobaghdad.edu.iq, amalsa_comp@csw.uobaghdad.edu.iq, wildanjh_comp@csw.uobaghdad.edu.iq, sahar.m@csw.uobaghdad.edu.iq,ammarhj_comp@csw.uobaghdad.edu.iq*

[b] *AL al-Bayt University, Jordan .Email: aligah.2020@gmail.com*

ARTICLE INFO

Article history:
Received: 20/08/2025
Rrevised form: 28/10/2025
Accepted : 02 /11/2025
Available online: 30/12/2025

Keywords:

Internet of Things, Cybersecurity, Threats, Challenges, Countermeasures.

ABSTRACT

The technology of connecting physical objects and devices to the Internet is called the Internet of Things[IoT]. With this technology, it has become possible to live within a smart environment that provides users with comfort, entertainment, and ease of doing business in various fields, including industry, medicine, energy, and even urban settings. Although this technology is a breakthrough in the field of communication and data exchange, it is not isolated from the challenges of cybersecurity. It is necessary to not forget that everything connected to the internet is vulnerable to hacking. Therefore, it is essential to rely on cybersecurity technologies and apply them to IoT systems to protect infrastructure and sensitive data from hacking. It's important to note that traditional security measures don't work effectively with IoT systems. Therefore, such systems require highly accurate and efficient protection systems, as security risks can put companies, governments, and even individuals at risk. Therefore, it's essential to develop strategies to combat cybersecurity crimes. To understand the most important challenges and opportunities within cybersecurity management, the paper discussed them in this article.

MSC..

https://doi.org/ 10.29304/jqcsm.2025.17.42555

1. Introduction

To begin with, the Internet of Things can be defined as a network of living devices that depends on and that can facilitate our lifestyles. It consists of physical devices [home appliances, vehicles, mechatronic and healthcare systems, software, embedded electronics, sensors, actuators, and others] that enable them to exchange data and communications [1], and this is the main goal of the Internet of Things, to integrate the digital and physical worlds into a unified system [2].

The Internet of Things is entering many areas of life, creating numerous job opportunities. An example of this is the smart factory, which is one of the most important applications of the Internet of Things. This application enables the user to distinguish between four components: the process, the smart object, the person, and the technological

∗Corresponding author Dr. Wildan Jameel Hadi

Email addresses: *wildanjh_comp@csw.uobaghdad.edu.iq*

Communicated by 'sub etitor'

ecosystem [2,3]. The close connection between digital manufacturing and the Internet of Things has helped achieve higher-quality products at lower costs. This includes big data analysis, advanced robotics, the Industrial Internet of Things, and cloud computing [4].

The Internet of Things faces numerous challenges, particularly those related to security, due to the large number of devices and complex environment. The term of cybersecurity is synonymous with IOT. That came to protect information, which encompasses many aspects such as information security, confidentiality, and access to that information [5]. Therefore, cybersecurity can be defined as the process of protecting network systems, computers, and data from unauthorized access, data disruption, theft, or manipulation [modification, use, or disclosure] [6]. The most important factors on which cybersecurity depends are protection methods [for information technology, real data, post-processing data], the level of protection after implementing these methods, and other professional aspects related to the protection methods [5]. Therefore, the true measure of cybersecurity is data accessibility, security, integration, transmission across various media, and storage methods [5] [7].

From here, the papers [8] [9] offered another definition of cybersecurity: It represents the methods and technologies that protect devices, networks, programs, and data from damage, unauthorized access, or attack. Cybersecurity covers several areas, including application security, which protects programs and devices from electronic threats and risks; network security, which protects networks from cyberattacks and hackers and prevents them from accessing computer networks; information security, which refers to the security and privacy of data; and operational security, which focuses on protecting data handling.

One of the most important challenges facing or threatening an Internet of Things project is data security and privacy [10]. Cybersecurity, or information technology security, is essential to protecting the data of Internet of Things systems and critical infrastructure. Therefore, one of the tasks of cybersecurity is to understand all aspects of cyberattacks and develop countermeasures to maintain the security, integrity, availability and confidentiality of data and information and digital technologies [9] [11] [12].

This study will focus on understanding contemporary cybersecurity from a comprehensive perspective to help both academics and employers. This research will contribute to the following: first, identifying and recognizing cybersecurity risks will include the details of risks, second, analyzing cybersecurity strategies to mitigate threats, and third, trends changing cyber security.

2.The Concept of Cybersecurity

Cybersecurity plays a crucial role in protecting information, whether personal, corporate, or national security information [13]. With the continued advancement of technology, the threats used by cybercriminals have evolved, making cybersecurity more important than ever [14].

Cybersecurity systems have the ability to protect data, computers, and networks from hacking, unauthorized access, and all other attacks that may include modification, alteration, and destruction[3] [4][15]. This requires significant measures to mitigate, detect, and prevent such threats, whether malware, ransomware, phishing attacks, or others [16]. Cybersecurity secures these devices, networks, and data, in addition to educating users [17]. This is achieved by implementing security tools and all policies to ensure availability, integrity and confidentiality of information and systems[13] [15] [16].

On the other hand, the widespread use of technology and the internet has significantly increased the incidence of cyber-attacks and data breaches, which can cause significant damage to organizations and individuals alike. Including financial losses, loss of life, damage to reputation, or the overthrow of government and international figures in some cases [18] [19].

The internet has given each of us our digital world, through communicating with others, shopping online, or setting up bank accounts. All these things are done online, making a person's information and interactions within their environment vulnerable to cyberattacks [2] [8] [20].

Cybersecurity is also crucial to increasing confidence and trust in digital security[9]. Consumers need to feel secure about the safety of their information, given the massive volume of financial transactions and e-commerce [21]. Therefore, cybersecurity technologies are of great importance to the continued effectiveness of businesses and governments, including consumers, in conducting their business online. Otherwise, it becomes difficult to sustain economic growth [22].

Cybersecurity systems prevent hackers and cybercriminals from exploiting vulnerabilities and gaining unauthorized access to sensitive data[23] . Common threats include intellectual property theft, malicious access to sensitive information, fraud in financial and banking transactions, infrastructure disruption, and many more. These systems protect consumers from their data and all their digital transactions falling into the wrong hands and being exploited by cybercriminals [23] [24].

In addition to protecting consumers and their information, cybersecurity is crucial for businesses and organizations and their information [25]. Cyberattacks can result in financial losses or damage to an organization's reputation. Through cybersecurity measures, organizations can prevent or detect such breaches before they are too late, thereby mitigating the potential impact of such breaches [26].

3.Management of Cybersecurity Risks

The risks posed by a network attack or intrusion depend on three important factors: threats, vulnerabilities, and attacks. To understand what these factors are and how they relate to attacks, there are some concepts [25] [26] [27] [28]:

Cyberspace: Within the world of information, there is a global domain called cyberspace. To create, store, update, and share information, cyberspace utilizes the electromagnetic and electronic spectrum, aided by the latest information and communications technologies within interconnected networks.

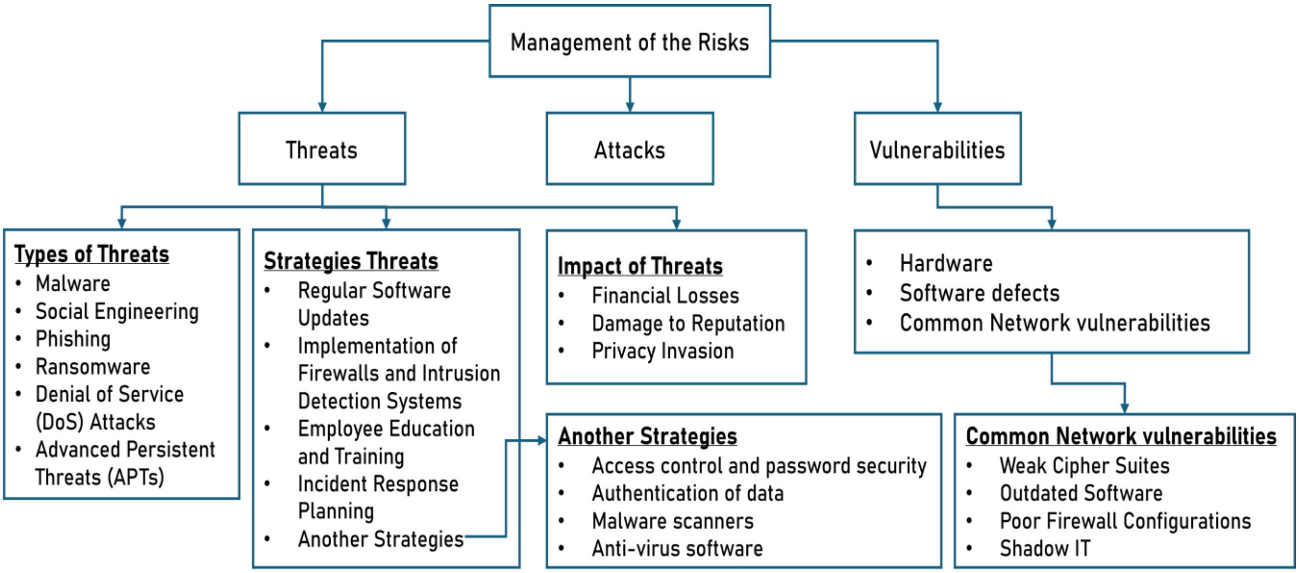
vulnerabilities: Most attacks rely on flaws or vulnerabilities in the system, which allow attackers to exploit them to execute malicious commands, gain unauthorized access to the system, or launch denial-of-service attacks.

Threats: These are the operations or actions carried out by an attacker to exploit security breaches in the system and negatively affect it.

Attacks: These are measures used to disrupt or destroy routine system operations by exploiting existing vulnerabilities and weaknesses on it, using various techniques and tools. Attacks are then launched to achieve malicious goals in exchange for financial rewards or personal gratification.

There are some concepts and terms related to cybersecurity that researchers should be familiar with [29] [30] [31] [32]. The study describes them in table 1:

Table 1 Management of Cybersecurity Risks



3.1Threats

3.1.1 What Are the Threats?

With the development of technology and the emergence of the digital world, cybersecurity threats have become a major concern, especially with the increase in these threats [33]. The individuals who actually or possibly succeed in cyberattacks are frequently cited as getting into at least one of five classifications [33] [34] [35]:

Spies seeking to obtain confidential and sensitive data targeting government or private entities; hacktivists carrying out cyberattacks for non-financial reasons; terrorists participating in cyberattacks to destabilize the security of the targeted state as a form of warfare; the defendant's intent to profit from fraud and falsification of information and Nation-state combatants develop capabilities and undertake cyberattacks to support the country's strategic objectives. Here's a summary of cybersecurity threats:

3.1.2 Types of Cybersecurity Threats

Different types of threat that affect cybersecurity as shown in the figure 1

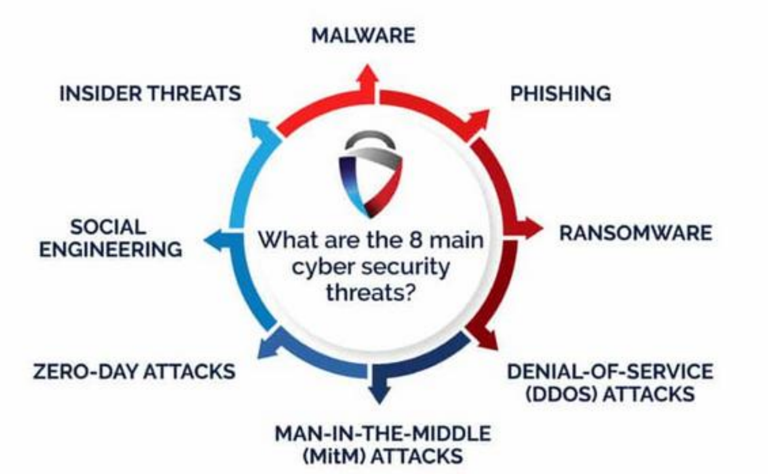

MALWARE
INSIDER THREATS
PHISHING
What are the 8 main cyber security threats?
SOCIAL ENGINEERING
RANSOMWARE
ZERO-DAY ATTACKS
DENIAL-OF-SERVICE (DDOS) ATTACKS
MAN-IN-THE-MIDDLE (MitM) ATTACKS

Fig. 1 Type of Threat.

- **Malware**

Malware is software designed to harm a computer system or computer network. There are several types: worms, viruses, spyware, ransomware, Trojans and other dangerous types. It is typically transmitted by attached email, software downloads, compromised websites, or susceptible software. Malware, when placed on computer software, could steal the critical data, erase files, and allow unauthorized access to a network. Therefore, to protect computers from malware, it is essential to install powerful software to detect and combat malware and protect systems from such attacks [18] [19].

- **Social Engineering**

Attackers often use social engineering techniques to trick targets into accessing important information or putting them at risk [15] [18].

In[13] [28], they entail people's behavior and their trust to trick them into disclosing information, which might include passwords or financial details, also compel them into doing things that didn't do it in normal, like creating attachments to malicious email or clicking on links. Social engineering appears in more than one image [phishing emails, phone calls, people faking coworkers, IT staff, fake websites or social networking profiles] all this form to win confidence. Social engineering techniques can be used by attackers on individuals, like tailgating [following the victim into a secure area without sufficient authorization] and pretexting [making up a fictitious situation to acquire confidence and influence the victim into sharing information].

Social engineering attacks can have a variety of purposes, but they frequently involve identity theft, financial fraud, illegal access to networks, and the transmission of malware or ransomware. Protecting contra social engineering attacks involves education, awareness and suspicion [31] [34]. It is very important to be careful when discussing personal information to avoid it being exploited by unauthorized persons and creating security risks [1] [5].

To protect government institutions and companies from any attacks, it is essential to train their employees in social engineering techniques, how to recognize attacks, and how to implement security systems and protocols [37].

- **Phishing**

Phishing is a type of cybercrime in which attackers mimic a legitimate institution or organization, like a bank or provider of an internet service, to trick people into disclosing personal information [passwords, or credit card details] [24]. Phishing Commonly involves sending phishing messages or developing fake websites that look like authentic ones. The attacker has obtained access information that can be exploited to a variety of harmful objectives, this information includes theft identity and financial fraud [1] [16]. The individuals and organizations may be threatened by phishing attacks that try to be aware of phishing signs, such as unusual website URLs or unusual email requests. It will try to avoid been victim to these scams [37] [8].

- **Ransomware**

Ransomware is a type of malware that accesses the victim's files, encrypts them, and extorts the victim to pay a ransom to decrypt the files. The extortion may be directed at individuals or at institutions or companies [11]. The most common way ransomware infects the files of targeted individuals or companies is by exploiting a vulnerability in a computer system or specific software [14].

Most ransomware, after accessing and encrypting files, displays a warning message to the victim, telling them how to pay the ransom and giving them a deadline, threatening to permanently delete the files if the ransom is not paid [21].

- **Denial of Service [DoS] Attacks**

A DoS attack is one of cyber-attack types where a perpetrator purposefully floods the website, server, and network with too much traffic or data overloading its rendering and resources unavailable to users. The DoS attack aims to interrupt the normal operation of a target system or network and make it inaccessible [23].

In different ways DoS attacks can be used by including flooding targets with a large volume of network demands, using botnets [like sending spam messages] to flood the target with traffic from multiple sources, or to utilize a vulnerability in the target's infrastructure software [26].

To mitigate the impact of DoS attacks and minimize their effects on the affected companies, develop protocols to counter such attacks, limit their impact, and cooperate with law enforcement authorities to limit the effects of such attacks on stakeholders [33].

- **Advanced Persistent Threats [APTs]**

Advanced persistent threats are cyberattacks carried out by highly skilled hackers targeting government organizations to gain access to a specific system or sensitive data, often acting on behalf of a specific nation-state. Most of these attacks may last for a long time to achieve their goal [35].

APTs usually have several steps, including modifying or collecting important information, establishing bases, moving laterally via the network, original reconnaissance and penetration [31] [38]. To avoid detection, attackers use complex techniques such as bespoke malware, zero-day weaknesses, and social engineering. The motivation for APTs vary, but they typically involve gathering information, stealing propriety information, conducting illicit activity, or disrupting key infrastructure. Government entities, defense-related firms, companies involved in research and development corporations are common targets of such attacks, and financial institutions [35]. To fight against APTs, firms should put in place comprehensive security measures, including perfect access controls, network segmentation, regular vulnerability assessments, and training staff on best practices of security [2] [3] [13].

3.1.3 The Harmful Effects of Cybersecurity Threats

A. Financial Losses

Recently, cybersecurity threats have had a significant impact on the financial aspects of both individual and organizational accounts [17]. These attacks can lead to access to sensitive banking information or unauthorized access to companies' financial systems, potentially leading to significant economic losses for individuals and businesses and potentially legal liability related to financial fraud [21]. On the other hand, cybersecurity attacks can disrupt certain programs for companies and institutions. These companies may therefore incur significant financial burdens, resulting in significant financial losses [23] [25]. They will need to intensify efforts to maintain revenue and compensate for losses, which adds further financial burdens [30].

Cybersecurity attacks also incur costs in legal fees and fines, as such cyber breaches often lead to investigations by the judicial authority [32]. Such breaches increase wages and financial pressure on the targeted organizations and companies, which require the appointment of legal counsel to handle cases related to cybersecurity breaches [7] [37].

Finally, cybersecurity attacks can indirectly cause financial losses for companies and organizations through the loss of customer trust. Such attacks can harm a company's reputation, leading to a decline in sales and draining the efforts of remaining customers. Focusing on rebuilding reputation and regaining customer trust requires additional costs and takes a long time [39].

B. Damage to Reputation

Cybersecurity technologies are crucial in enhancing customer trust in companies. Therefore, when a particular company is subjected to a breach, the company's reputation is at risk. Most cybersecurity attacks target sensitive customer data, which can erode trust and credibility between customers and organizations, leading to a loss of security [40]. These risks can damage a company's reputation and potentially lead to the loss of customers [34]. Furthermore, cybersecurity attacks not only impact a company's relationship with customers but also threaten its relationship with stakeholders. Most attacks leave companies and organizations unable to protect sensitive information, which can cause stakeholders to refrain from continuing business with such companies and thus lose financial support for the company [41].

Finally, cybersecurity attacks targeting a specific company or organization may make it an easy target for media scrutiny. This depends on how the organization or company responds to the breach and how it mitigates the situation with minimal losses and avoids media hype [34]. Failure to respond quickly and address cyberattacks wisely may result in the company losing its reputation and, consequently, public trust. Such damage to a company's reputation can have long-term repercussions, and it is difficult to erode customer and company trust in the short term, as this requires effective cybersecurity measures and efforts to prevent the company from becoming an easy target for such attacks [33] [40].

C. Privacy Invasion

Privacy violations caused by cybersecurity attacks have become increasingly prevalent recently, with most of these attacks involving financial fraud, access to bank accounts, or theft of credit card information, which can have severe financial and emotional consequences for individuals and their families [41].

Privacy breaches can have repercussions for companies, especially startups, including privacy breaches of customer information, personal data, and the company's trade and financial secrets. Such breaches can cost the company financial losses and lead to legal action [40] [41.

Privacy invasions have dimensions beyond financial consequences: they include people losing trust in the digital environment, undermining personal freedoms, and avoiding completing tasks and business online and through social media. All of these dimensions can hinder the growth of the digital economy [29].

3.1.4 Strategies to Minimize Cybersecurity Threats

A. Structured Software Updates

The software update and security patches are the most effective strategies to lessen cybersecurity threats. This software may contain bugs and vulnerabilities that could be utilized by hackers, so many updated programs were released by software developers all the time that made the users comfortable with the protected software and all information [2].

The users must always install operating systems and software updates to close any security loopholes that can be easily exploited by cybercriminals who are always evolving their tactics and techniques [43].

One of the software updates' characteristics is to fix bugs and improve overall system performance, which makes it easier for users to complete their work on their applications without worrying about system downtime or data loss [40] [41].

All modern programs have the feature of automatic or manual updating. This feature must be followed because it ensures that security patches are installed in the programs to protect against attacks [37].

The user must pay attention to regularly updating your operating system, antivirus software, internet browsers, and other similar programs to avoid any security vulnerabilities that could be hacked [42].

B. Implementation of Firewalls and Intrusion Detection Systems

Most organizations create a railing between their internal network and the external internet by implementing a type of network security device called a firewall, whose goal is to prevent unauthorized access and protect sensitive data, and monitor incoming and outgoing network traffic [44]. Recently, Intrusion Detection Systems [IDS] have appeared that are software or hardware-based systems that monitor network traffic for suspicious and malicious activity. They analyze network packets and patterns to detect irregularity and possible security breaches and

Making security administrators fully aware, allowing them to use immediate measures to reduce the threat [45]. All organizations' goals are identifying and blocking potential threats before they can cause harm to software, so they use firewalls and IDS that provide security by using an additional layer of protection against cyber-attacks [45]. This layer controls access to the network and detects and responds to suspicious activity [46]. To mitigate cybersecurity attacks and reduce losses at all levels, organizations must periodically update their security systems, test their effectiveness, and review and monitor logs in case of tampering. The methods used to enhance the security and protection system have become clear to individuals through choosing strong passwords or using multi-layered encryption algorithms to protect sensitive data, as well as training employees to update cybersecurity defenses frequently and implementing other practices to implement a strong security approach in institutions [45].

Cybersecurity is a technology that requires staying up-to-date with the latest updates to stay safe against threats. This means organizations must constantly update their security systems and train their employees [47].

C. Regular employee training

All organizations must educate and train employees to combat cybersecurity attacks by combating electronic fraud, avoiding weak passwords, and not using untrusted websites. This, in turn, improves employee skills [48].

The subject matter of training sessions can include how to identify phishing emails, use strong passwords, two-factor authentication, and the risks associated with downloading or clicking on unknown links or attachments. Also, these training sessions keep employees informed of the latest cybersecurity threats, the technologies they use, and how to counter them as much as possible [49]. So, they will be educated on the potential consequences of a cybersecurity breach, both for their individual information and for the overall security of the company [48].

The multimedia has major roles in providing informational resources that help employees keep informed about new threats and provide advice for staying safe online [49]. Also, the employees are responsible for quickly noticing any unusual and potentially dangerous to alert IT or security teams if they suspect a breach or suspicious activity. On the other hand, providing a safe environment for employees to ask questions and report without fear in the event of any security breach [50].

using the simulated phishing attacks to measure employees' knowledge and their readiness, so those who oversee these training programs can determine the areas of weakness [51].

D. Incident Response Planning

All organizations must have an incident response plan when a cybersecurity incident happens [41] [52]:

- Find out the cause of the accident.
- Controlling the incident to avoid as many losses as possible.
- Taking possible precautions to prevent a recurrence.
- Responding quickly to the incident and notifying stakeholders to avoid data loss.

The advantages of having an incident response plan are [28] [33]:

- Systematically updating security systems is crucial to keeping pace with changes.
- Preventing attacks as they occur helps the organization avoid losses.
- Train employees on how to respond in the event of an attack.
- Attempt to prevent attacks as much as possible.

E. Another Strategies

- **Access control and password security**

Using the username and password has been a fundamental way of protecting personal information. This may be one of the first measures regarding cyber security [40].

- **Authentication of data**

The user device must have good anti-virus software to protect the device from viruses. Also, all received documents must be authenticated before downloading by using the anti-virus software present on the devices [39].

- **Malware programs**

It is a program that scans the computer system for any malicious files or software, such as Trojan horses, viruses, worms, and others [32].

- **Anti-virus programs**

Antivirus programs are very important programs in any computer system because they have the ability to detect and identify malicious programs and then treat them [32] [34].

The following table shows comparison between strategies that reduce or mitigate threats:

Table 2: C omparison ofS trategies toMitigate C ybersecurityThreats

Strategy	Benefit	Threats Mitigated
Structured Software Updates	Fixes bugs and vulnerabilities, improves system stability, closes security loopholes.	Malware, Ransomware, APTs
Firewalls & Intrusion Detection Systems [IDS]	Prevents unauthorized access; monitors suspicious traffic; adds an extra layer of protection.	DoS/DDoS Attacks, Malware, APTs
Regular Employee Training	Raises awareness; reduces human errors; helps identify phishing & social engineering	Social Engineering, Phishing, Ransomware

	attempts.	
Incident Response Planning	Ensures quick detection, containment, and recovery; minimizes losses; prevents recurrence.	APTs, DoS/DDoS Attacks, Malware
Access Control & Strong Passwords	Limits unauthorized access; protects sensitive accounts and systems.	Social Engineering, Phishing, Insider Threats
Antivirus & Anti-Malware Programs	Detects, blocks, and removes malicious software before it spreads.	Malware, Ransomware, Trojans, Worms

3.2 Vulnerabilities

3.2.1 What Are the Vulnerabilities?

Cybersecurity is essentially an arms race involving attackers and defenders. ICT systems are extremely complex, and attackers are continuously looking for flaws, which can appear at any point. Defenders can often prevent weaknesses, but all three are particularly difficult: inadvertent or deliberate activities by insiders with system access; supply-side vulnerabilities, which allow the insertion of illicit hardware or software during acquisition procedures; and previously unidentified or zero-day vulnerabilities with no known fix. Even when remedies for vulnerabilities are identified, they are often not implemented due to budgetary or operational restrictions [43].

Once malware is installed on the victim's system, cybercriminals can exploit a variety of existing vulnerabilities in the victim's system to enhance their illegal activities. The study investigates the most widely exploited vulnerabilities in software, hardware, and network systems [47].

A. Hardware

Hardware is the most powerful entity capable of affecting a computer system. Unlike software attacks, many hardware-based attacks cannot be detected. Hardware-based attacks are on the rise, due to the lack of supporting tools to detect them [49].

Illegal device copies have become a source of hardware-based exploitation, with the potential for illegally counterfeiting devices, including malicious vulnerabilities or Trojans, becoming increasingly possible. The potential for counterfeit devices has increased because of a new trend in IT organizations attempting to cut costs by outsourcing and purchasing unreliable equipment from online sources [51].

Similarly, it is noted that IT organizations often purchase unreliable equipment, such as processors and routers, through auction sites or resellers, which may contain dangerous Trojans. These actions are not only troublesome for IT organizations that operate on altered hardware that might enable backdoor entry, but they also raise the likelihood that the original design and details of the system's internal states would be revealed to unauthorized individuals. Side-channel attacks occur when adversaries obtain information about a system's internal states by examining the device's physical characteristics, such as power usage, electromagnetic radiation, and data in and out time [50].

Side-channel attacks can result in the leakage of sensitive data. describes an approach that investigates how the secret key of a cryptographic algorithm can be revealed because of radio frequency analysis [51].

B. Software defects

A software bug is a common term to describe a mistake, defect, or problem in a computer program, such as an operating system, external input/output interface drivers, and applications. Cyberattacks exploit software vulnerabilities to force systems to behave in unexpected ways that deviate from their original design [49]. Most of the current cyberattacks still involve exploiting software vulnerabilities caused by software flaws and design errors [47].

Exploits target the software stacks and interfaces. The most prevalent software vulnerabilities are caused by exploiting software defects in memory, input from individuals, validation, race situations, and user access rights [45].

Software engineers uncover frequent programming flaws that contribute to software vulnerabilities, create standard secure coding norms, educate those who develop software, and enhance the practice of secure coding. Language-based safe code practice involves developing strategies to make sure that programs do not breach important security standards [46].

Code obfuscation is the process of making source or machine language difficult for humans to understand. Programmers frequently purposely obfuscate code to obscure its purpose or logic and thwart reverse engineering attempts [44]. A secure conception and creation cycle was also put forward, which includes a set of design methodologies for efficiently verifying that a system element is without any potential faults from its conception. Though they are not simple approaches, formal methods allow you to thoroughly investigate the design and identify subtle security problems [44] [45]. Tools and procedures have been created to help verify mission-critical security attributes. These methods and instruments assist in translating higher-level security goals into a set of atomic qualities that can be validated [42].

C. Common Network vulnerabilities

Regularly scanning of the network and system infrastructure can uncover vulnerabilities in employees, encryption systems, or firewalls, which are often exploited by attackers as shown in figure 2[46] .

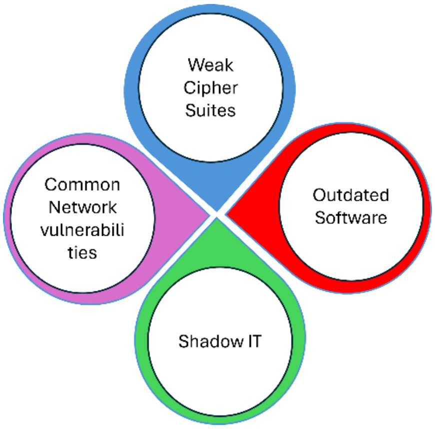


Fig. 2 Common Network vulnerabilities.

3.3 Attacks

Considering the digital advancements that are witnessing today, attackers have also become more sophisticated in their techniques in terms of reaching a greater number of targets. Attackers can be divided into several categories, including those who carry out attacks in search of money, credit card and banking information, and other information; another category targets computer resources for illegal purposes; and another category carries out attacks motivated by threats and the spread of chaos and terror [47] [48].

A successful attack can jeopardize the security, reliability, and accessibility of an ICT system and the data it processes. Cyber theft or cyber spying can lead to the transfer of financial, confidential, or personal information, often without the victim's awareness [42]. Denial-of-service attacks can cause genuine users to experience delays or be unable to use the system. Botnet malware allows an attacker to take control of a system and use it to launch cyberattacks on additional systems. Attacks on industrial automation systems can destroy or impair the equipment they manage, including generators, pumps, and centrifuges [46].

While it is widely acknowledged that cyberattacks are frequently costly to both individuals and businesses, the economic consequences can be hard to quantify, and estimates vary greatly. The annual cost of cybercrime to the world economy is commonly quoted at $400 billion, with some experts claiming that costs are rising significantly, particularly with the continuing expansion of information and communication technology via the Internet of Things, along with other new and developing platforms [2] [3]. The expenses of cyberespionage might be harder still to calculate but are regarded to be enormous.

Managing cyberattack risks typically entails [1] removing the threat sources [e.g., by shutting down botnets or lowering promotions for cybercriminals]; [2] focusing on vulnerabilities by hardening ICT assets [e.g., by repairing software and educating employees]; and [3] mitigating effects by mitigating damage and preserving functions [e.g., by having backup resources obtainable to ensure continuity of activities in response to an attack]. The ideal level of decreased risk will vary by sector and organization. Customers may expect lower levels of cybersecurity from an entertainment corporation than from a bank, hospital, or government organization [48] [50] [52].

4. Trends Changing Cyber Security

Some of the trends that have significantly impact on cybersecurity will be mentioned below.

4.1 Web servers:

The threat of attacks on web applications to extract data, spread destructive or malicious software still exists. Cybercriminals distribute their malware through legitimate web servers until they are compromised [53]. Due to the frequent attacks targeting data in general, which attract press and media attention, it has become important to focus on web servers and provide high-security systems to prevent cybercriminals from accessing and manipulating data [56].

4.2 Cloud computing and its services

Today, all small, medium, and large companies rely on cloud computing services. In other words, the world is gradually moving toward cloud computing. This latest trend poses a significant cybersecurity challenge, as data traffic can go around traditional checkpoints [54]. With the significant increase in cloud computing applications, his has also led to the development of policy controls for web applications and cloud services to prevent the loss and tampering of valuable information. Although cloud services are evolving, many security issues still arise. Cloud computing may offer tremendous opportunities, but it's important to note that as it evolves, so too do security concerns [56].

4.3 APT's and targeted attacks

Advanced Professional [APT] is constantly in demand at a whole new level within cybercrime ware, and network security skills, such as web filtering or an Intrusion Prevention System [IPS], play a partial part in detecting these targeted elements [mostly after the initial compromise]. As attackers' techniques evolve and adopt more sophisticated methods, it has become necessary to implement an integrated security system that includes network security, software security, and systems security simultaneously [57].

4.4 Mobile Networks

Today, connectivity is available to anyone, anywhere in the world. However, the security of mobile networks is a concern for people. These days, firewalls and other security measures are becoming porous as people to use, such as tablets, phones, and other personal computers, all etc. all of which again require extra security apart from those present in the applications used. An equally important point that requires a protection system is mobile networks, as they are more vulnerable to attackers [54] [57].

4.5. Encryption of the code

Encryption is the process of writing and encoding messages [or information] in a way that prevents eavesdroppers or hackers from identifying or reading them. In a cryptographic system, the message or information is encrypted using cryptographic algorithms, converting it into cipher text that is unreadable or incomprehensible [55]. This is typically done using an encryption key that specifies how the message is encoded. At its most basic level, encryption protects the privacy and integrity of the data. However, the widespread use of encryption will bring more challenges in the field of cybersecurity [54]. Encryption is also used to protect data during transmission, for example, data transmitted over networks [such as the Internet and e-commerce], mobile phones, wireless microphones, wireless intercoms, etc. Hence by encrypting the code, one can know if there is any leakage of information [56].

5. Conclusion

The Internet of Things [IoT] faces significant security challenges as it has become the primary tool for protecting networks, data, and infrastructure from various external threats [software, ransomware, phishing, advanced persistent threats, and denial-of-service attacks]. The study found that cyberattacks have gone beyond financial losses to long-term damage [reputational damage, decreased customer trust, and privacy breaches].

Cybersecurity therefore requires a proactive approachs that combines firewalls, regular software updates, employee training, intrusion detection systems, and well-prepared incident response plans. Addressing vulnerabilities in software, hardware, and networks is also essential to mitigating and reducing risk. This requires governments and organizations to continuously monitor their defense strategies, given their reliance on web services, cloud computing, and the Internet of Things.

Cybersecurity is therefore a vital component of maintaining trust, enabling secure digital growth, and ensuring business continuity. This has led to cybersecurity being constantly enhanced to address evolving threats and secure the future of digital transformation.

References

[1] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, “Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework,” Jul. 01, 2024, *Multidisciplinary Digital Publishing Institute [MDPI]*. doi: 10.3390/app14135501.

[2] M. Homaei, Ó. Mogollón-Gutiérrez, J. C. Sancho, M. Ávila, and A. Caro, “A review of digital twins and their application in cybersecurity based on artificial intelligence,” *Artif Intell Rev*, vol. 57, no. 8, Aug. 2024, doi: 10.1007/s10462-024-10805-3.

[3] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, “Cybersecurity challenges in vehicular communications,” Jun. 01, 2020, *Elsevier Inc.* doi: 10.1016/j.vehcom.2019.100214.

[4] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, “Advancing cybersecurity: a comprehensive review of AI-driven detection techniques,” *J Big Data*, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-024-00957-y.

[5] L. Ofusori, T. Bokaba, and S. Mhlongo, “Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction,” *Applied Artificial Intelligence*, vol. 38, no. 1, 2024, doi: 10.1080/08839514.2024.2439609.

[6] Z. M. King, D. S. Henshel, L. Flora, M. G. Cains, B. Hoffman, and C. Sample, “Characterizing and measuring maliciousness for cybersecurity risk assessment,” Feb. 05, 2018, *Frontiers Media S.A.* doi: 10.3389/fpsyg.2018.00039.

[7] S. L. Garfinkel, “Inside risks the cybersecurity risk,” Jun. 2012. doi: 10.1145/2184319.2184330.

[8] M. L, M. E, and M. A, “Cybersecurity Management for [Industrial] Internet of Things: Challenges and Opportunities,” *J Inf Technol Softw Eng*, vol. 08, no. 05, 2018, doi: 10.4172/2165-7866.1000250.

[9] M. Toussaint, S. Krima, and H. Panetto, “Industry 4.0 data security: A cybersecurity frameworks review,” May 01, 2024, *Elsevier B.V.* doi: 10.1016/j.jii.2024.100604.

[10] C. Florackis, C. Louca, R. Michaely, and M. Weber, “NBER WORKING PAPER SERIES CYBERSECURITY RISK,” 2020. [Online]. Available: http://www.nber.org/papers/w28196

[11] M. L, M. E, and M. A, “Cybersecurity Management for [Industrial] Internet of Things: Challenges and Opportunities,” *J Inf Technol Softw Eng*, vol. 08, no. 05, 2018, doi: 10.4172/2165-7866.1000250.

[12] K. Thakur, M. Qiu, K. Gai, and M. L. Ali, “An Investigation on Cyber Security Threats and Security Models,” in *Proceedings - 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 - IEEE International Symposium of Smart Cloud, IEEE SSC 2015*, Institute of Electrical and Electronics Engineers Inc., Jan. 2016, pp. 307–311. doi: 10.1109/CSCloud.2015.71.

[13] A. M. Alenezi, “BEYOND THE CLOUDS: INVESTIGATING DIGITAL CRIMES IN CLOUD ENVIRONMENTS A PREPRINT,” 2024.

[14] S. Muneam, M. Q. Jawad, and D. Hassan, “Survey and comparison of different classification techniques for select appropriate classifier of image,” vol. 7, no. 3, pp. 1396–1404, 2019, [Online]. Available: http://pen.ius.edu.ba

[15] A. M. Alenezi, “BEYOND THE CLOUDS: INVESTIGATING DIGITAL CRIMES IN CLOUD ENVIRONMENTS A PREPRINT,” 2024.

[16] A. M. Alenezi, “BEYOND THE CLOUDS: INVESTIGATING DIGITAL CRIMES IN CLOUD ENVIRONMENTS A PREPRINT,” 2024.

[17] A. M. Alenezi, “BEYOND THE CLOUDS: INVESTIGATING DIGITAL CRIMES IN CLOUD ENVIRONMENTS A PREPRINT,” 2024.

[18] A. M. Alenezi, “BEYOND THE CLOUDS: INVESTIGATING DIGITAL CRIMES IN CLOUD ENVIRONMENTS A PREPRINT,” 2024.

[19] D. Trninić, A. K. Vukelić, and J. Bokan, “Perception of ‘fake news’ and potentially manipulative content in digital media—a generational approach,” *Societies*, vol. 12, no. 1, Feb. 2022, doi: 10.3390/soc12010003.

[20] A. M. Alenezi, “BEYOND THE CLOUDS: INVESTIGATING DIGITAL CRIMES IN CLOUD ENVIRONMENTS A PREPRINT,” 2024.

[21] A. M. Alenezi, “BEYOND THE CLOUDS: INVESTIGATING DIGITAL CRIMES IN CLOUD ENVIRONMENTS A PREPRINT,” 2024.

[22] M. Pinto and S. Ferreira, "Development of a Website for Creation of Vulnerability Datasets."

[23] N. Mpekoa, "An Analysis of Cybersecurity Architectures."

[24] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," in *Journal of Computer and System Sciences*, Academic Press Inc., 2014, pp. 973–993. doi: 10.1016/j.jcss.2014.02.005.

[25] S. M. Dickson and I. P. OKECHUKWU, "Cyber Security in the Age of the Internet of Things, Constraints, and Solutions," *JOURNAL OF DIGITAL LEARNING AND DISTANCE EDUCATION*, vol. 2, no. 11, pp. 829–837, Apr. 2023, doi: 10.56778/jdlde.v2i11.233.

[26] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," Feb. 01, 2021, *MDPI AG*. doi: 10.3390/fi13020039.

[27] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," Feb. 01, 2021, *MDPI AG*. doi: 10.3390/fi13020039.

[28] W. J. Hadi, S. M. Kadhem, and A. R. Abbas, "Fast discrimination of fake video manipulation," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 3, pp. 2582–2587, Jun. 2022, doi: 10.11591/ijece.v12i3.pp2582-2587.

[29] W. J. Hadi, S. M. Kadhem, and A. R. Abbas, "A survey of deepfakes in terms of deep learning and multimedia forensics," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 4, pp. 4408–4414, Aug. 2022, doi: 10.11591/ijece.v12i4.pp4408-4414.

[30] I. Lee, "Cybersecurity: Risk management framework and investment cost analysis," *Bus Horiz*, vol. 64, no. 5, pp. 659–671, Sep. 2021, doi: 10.1016/j.bushor.2021.02.022.

[31] T. Oluwaseun Abrahams *et al.*, "MASTERING COMPLIANCE: A COMPREHENSIVE REVIEW OF REGULATORY FRAMEWORKS IN ACCOUNTING AND CYBERSECURITY," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 120–140, 2024, doi: 10.51594/csitrj.v5i.709.

[32] T. Oluwaseun Abrahams *et al.*, "MASTERING COMPLIANCE: A COMPREHENSIVE REVIEW OF REGULATORY FRAMEWORKS IN ACCOUNTING AND CYBERSECURITY," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 120–140, 2024, doi: 10.51594/csitrj.v5i.709.

[33] G. N. Reddy and G. J. U. Reddy, "A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES."

[34] T. Oluwaseun Abrahams *et al.*, "CYBERSECURITY AWARENESS AND EDUCATION PROGRAMS: A REVIEW OF EMPLOYEE ENGAGEMENT AND ACCOUNTABILITY," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 100–119, 2024, doi: 10.51594/csitrj.v5i.708.

[35] J. Kaplan, S. Sharma, and A. Weinberg, "Meeting the cybersecurity challenge."

[36] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arab J Sci Eng*, vol. 45, no. 4, pp. 3171–3189, Apr. 2020, doi: 10.1007/s13369-019-04319-2.

[37] C. Maraveas, M. Rajarajan, K. G. Arvanitis, and A. Vatsanidou, "Cybersecurity threats and mitigation measures in agriculture 4.0 and 5.0," Dec. 01, 2024, *Elsevier B.V.* doi: 10.1016/j.atech.2024.100616.

[38] E. A. Fischer, "Cybersecurity Issues and Challenges: In Brief," 2016. [Online]. Available: www.crs.gov

[39] I. Kumar, "Emerging Threats in Cybersecurity: A Review Article," 2023. [Online]. Available: http://bluemarkpublishers.com/index.php/IJANS

[40] A. Zineddine *et al.*, "A systematic review of cybersecurity assessment methods for HTTPS," *Computers and Electrical Engineering*, vol. 115, Apr. 2024, doi: 10.1016/j.compeleceng.2024.109137.

[41] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review," Sep. 01, 2022, *Multidisciplinary Digital Publishing Institute [MDPI]*. doi: 10.3390/jcp2030027.

[42] A. Shahana *et al.*, "AI-Driven Cybersecurity: Balancing Advancements and Safeguards," 2024, doi: 10.32996/jcsts.

[43] J. Rahim, M. Ihsan, I. Rahim, A. Afroz, and O. Akinola, "Cybersecurity Threats in Healthcare IT: Challenges, Risks, and Mitigation Strategies", doi: 10.60087.

[44] I. Jada and T. O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," *Data Inf Manag*, vol. 8, no. 2, Jun. 2024, doi: 10.1016/j.dim.2023.100063.

[45] Adebola Folorunso, Temitope Adewumi, Adeola Adewa, Roy Okonkwo, and Tayo Nathaniel Olawumi, "Impact of AI on cybersecurity and security compliance," *Global Journal of Engineering and Technology Advances*, vol. 21, no. 1, pp. 167–184, Oct. 2024, doi: 10.30574/gjeta.2024.21.1.0193.

[46] "Assessing the Effects of Cyber Attacks on Financial Markets", doi: 10.60087.

[47] Philip Olaseni Shoetan, Olukunle Oladipupo Amoo, Enyinaya Stefano Okafor, and Oluwabukunmi Latifat Olorunfemi, "SYNTHESIZING AI'S IMPACT ON CYBERSECURITY IN TELECOMMUNICATIONS: A CONCEPTUAL FRAMEWORK," *Computer Science & IT Research Journal*, vol. 5, no. 3, pp. 594–605, Mar. 2024, doi: 10.51594/csitrj.v5i3.908.

[48] Adedoyin Tolulope Oyewole, Chinwe Chinazo Okoye, Onyeka Chrisanctus Ofodile, and Chinonye Esther Ugochukwu, "Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio," *World Journal of Advanced Research and Reviews*, vol. 21, no. 3, pp. 625–643, Mar. 2024, doi: 10.30574/wjarr.2024.21.3.0707.

[49] O. Gulyas and G. Kiss, "Impact of cyber-Attacks on the financial institutions," in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 84–90. doi: 10.1016/j.procs.2023.01.267.

[50] N. N. Cele and S. Kwenda, "Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review," Jan. 23, 2025, *Emerald Publishing*. doi: 10.1108/JFC-10-2023-0263.

[51] D. Ghelani, "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review," Sep. 22, 2022. doi: 10.22541/au.166385207.73483369/v1.

[52] F. Alharbi *et al.*, "The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia," *Sensors*, vol. 21, no. 20, Oct. 2021, doi: 10.3390/s21206901.

[53] A. I. Mallick and R. Nath, “Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments”, [Online]. Available: www.worldscientificnews.com

[54] S. Kumari, P. Pattanaik, and M. Zubair Khan, “Impact of Cybersecurity Measures in theHealthcare Sector: A Comprehensive Review ofContemporary Approaches and EmergingTrends,” *International Journal of Education and Management Engineering*, vol. 14, no. 6, pp. 1–19, Dec. 2024, doi: 10.5815/ijeme.2024.06.01.

[55] A. Kuzior, I. Tiutiunyk, A. Zielińska, and R. Kelemen, “Cybersecurity and cybercrime: Current trends and threats,” *Journal of International Studies*, vol. 17, no. 2, pp. 220–239, 2024, doi: 10.14254/2071-8330.2024/17-2/12.

[56] Olukunle Oladipupo Amoo, Akoh Atadoga, Femi Osasona, Temitayo Oluwaseun Abrahams, Benjamin Samson Ayinla, and Oluwatoyin Ajoke Farayola, “GDPR’s impact on cybersecurity: A review focusing on USA and European practices,” *International Journal of Science and Research Archive*, vol. 11, no. 1, pp. 1338–1347, Feb. 2024, doi: 10.30574/ijsra.2024.11.1.0220.

[57] A. S. George, “Emerging Trends in AI-Driven Cybersecurity: An In-Depth Analysis,” 2024, doi: 10.5281/zenodo.13333202.