Journal of Information Technology and Cyber Security 1(2) July 2023: 53-67 EISSN 2987-386X | PISSN 2987-3878
DOI: 10.30996/jitcs.9715

Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age

Akinul Islam Jony [1,*] and Sultanul Arifeen Hamim [2]

[1,2] Department of Computer Science, American International University-Bangladesh, Bangladesh
* Corresponding author: akinul@aiub.edu

Received: 23 October 2023
Accepted: 06 January 2024
Revised: 24 December 2023
Available online: 10 January 2024

To cite this article: Jony, A. I., & Hamim, S. A. (2023). Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age. *Journal of Information Technology and Cyber Security, 1*(2), 53-67. https://doi.org/10.30996/jitcs.9715

Abstract

In this contemporary digital age, cybersecurity stands as a crucial linchpin amid the expanding role of technology in our lives, encountering numerous challenges. This review addresses the imperative need for robust cybersecurity measures as malicious actors continually innovate methods to exploit vulnerabilities in computer systems, networks, and data. The exploration delves into the multifaceted realm of cybersecurity attacks, unveiling the evolving threat landscape and their profound implications. From cybercriminals utilizing phishing attacks to the covert tactics of malware and the disruptive potential of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, including Phishing, Zero-Day Exploits, Man-in-the-Middle, and SQL Injection Attacks, the cybersecurity battleground is ever-expanding. The study systematically categorizes cyber threats, scrutinizes their distinctive characteristics, and elucidates the modus operandi of each attack type. Through a meticulous dissection of cybercriminal methods and motivations and a comprehensive evaluation of countermeasure efficacy, this review offers indispensable insights for securing our digital future in an era marked by escalating interconnectivity and technological dependence.

Keywords: Attacks, cybersecurity, information security, systematic review, threats.

1. Introduction

In the modern age, where technological advances continually transform our daily lives, the digital realm has become an inextricable part of our existence. As Ghelani (2022) mentioned that immersion in the digital world promises unprecedented opportunities, redefining how we communicate, work, and socialize. Such transformative capabilities, however, come with a cost. As we have technology more profoundly into our social fabric, we expose ourselves to many potential risks, offering openings to malicious entities seeking to exploit our increased reliance on digital platforms (Muckin et al., 2019; Ulven & Wangen, 2021). These actors tirelessly innovate, continually evolving their methods to pierce through the defenses erected by cybersecurity experts, making the field of cybersecurity not just a technical imperative but a societal one.

The contemporary predicament revolves around the essence of digital progression. While it provides unparalleled convenience and interconnectedness, it also creates an expanding landscape of threats that becomes increasingly intricate daily (Abu et al., 2018). Cybercriminal activity has evolved from individual hackers operating in isolation to extensive networks comprising cybercrime syndicates and state-sponsored groups. Each actor possesses distinct goals, techniques, and resources at their disposal, resulting in a diverse array of threats that pose significant challenges to the fundamental integrity of our digital infrastructure (McGuire & Dowling, 2013). These malevolent groups employ many strategies, including phishing malware and advanced persistent threats, to exploit systems' vulnerabilities, often resulting in significant and widespread consequences. According to Hayzelden et al. (1999), the primary difficulty lies in ensuring the security of Information Technology and the associated data and consistently evaluating the efficacy of these protective measures.

A comprehensive understanding of the cyber threat landscape becomes paramount to navigating this intricate web of threats and vulnerabilities. It is not merely about countering individual threats but about

constructing an overarching strategy encompassing risk assessment, proactive defense, early detection, rapid response, and resilience-building (Brown et al., 2015; Schlette et al., 2021). By dissecting cyber adversaries' strategies, motivations, and methodologies, experts can refine their defense mechanisms, ensuring the security of data and the trust that society places in digital systems. This comprehensive approach, which balances technical acumen with strategic insight, offers a blueprint for surviving in the digital age and thriving amidst its complexities (Cavelty, 2010).

This study delves into the comprehensive domain of cybersecurity. It starts by categorizing various cyber threats, highlighting their distinct characteristics and tactics. Besides, it explores the motivations driving cybercriminals, giving insight into their objectives and strategies. Moreover, it evaluates defensive measures, assessing their efficacy and spotlighting standout strategies; an examination is conducted to investigate the underlying motives that propel individuals involved in cybercriminal activities, thereby providing insight into their specific goals and tactics. Subsequently, the investigation's focus transitions towards examining countermeasures, assessing their effectiveness and emphasizing exemplary approaches. By weaving together these different threads, this article aims to present a coherent narrative that underscores the importance, challenges, and solutions in navigating the cyber threat landscape of the digital age.

2. Background Study

In today's rapidly evolving digital landscape, cybersecurity is an ever-adapting sentinel, guarding the gates of sensitive information and vital infrastructure against an increasingly complex and pervasive array of threats. As we navigate the digital frontier, cyber-attacks have transcended traditional boundaries, manifesting as intricate, multifaceted operations that blend the elements of electronic warfare, psychological manipulation, computer network manoeuvring, military subterfuge, and robust security measures (Hart et al., 2020; Hawamleh et al., 2020). These orchestrated campaigns are designed to infiltrate and disrupt, compromise, or even manipulate the decision-making processes that govern our national institutions.

At the heart of this cyber battleground lie the intricate machinations of computer network operations—a trinity comprising attack, defence, and utilization (Ma et al., 2021). While network attacks and defences have long been recognized components of this digital theatre, the nuanced realm of utilization enabling operations beckons exploration. Here, the focus is squarely on gathering and analysing information, often serving as the harbinger of more disruptive actions yet to come (Thomson, 2015). These operations are not confined to mere data collection; they may also involve strategically disseminating information and propaganda, each makeover serving its unique purpose in the unfolding digital theatres (Alghamdi, 2021). In cybersecurity, the motivations behind cyber-attacks can vary widely, and one particularly concerning objective is the theft of crucial computer data. Within this context, a clandestine tool arsenal emerges as invaluable cyber espionage assets. Among these tools are Trap Sniffers and Doors, as highlighted by Liu et al. (2021). These covert instruments serve as the digital sleuths of the cyber world, allowing malicious actors to surreptitiously infiltrate systems and networks, all with the ultimate aim of pilfering sensitive and vital data. As the cyber landscape continues to evolve, deploying these tools underscores the critical need for robust cybersecurity measures to defend against the ever-present threat of data breaches and theft in our increasingly digitalized world (McCarthy et al., 2022). The particular concern amidst these evolving strategies is computer network exploitation, enabling operations of stealthy endeavours aimed at pilfering vital data from unsuspecting targets. In this intricate dance of cyber espionage, tools such as Trap Doors and Sniffers come to the forefront as critical actors (Furnell & Shah, 2020). The enigmatic Trap Doors provide external users with surreptitious access to software, all without the knowledge or consent of the primary user—a clandestine gateway into the heart of digital systems (Karbasi & Farhadi, 2021). In tandem, Sniffers ply their trade by covertly capturing the virtual footprints of unsuspecting users, seizing usernames and passwords in their relentless quest for sensitive information.

The US Department of Justice has categorized cybercrime into three primary classifications. The first category centres on manipulating the device itself, the second pertains to attacks employed as instruments against organizations, and the third involves incidents where a computer plays a supporting role in criminal acts (Mengidis et al., 2019). The focus of cybercriminal activities primarily revolves around these three defined areas. Cyberattacks can be executed through various methods, with some standard techniques encompassing Denial of Service (DoS) attacks, phishing attempts, identity theft, software piracy, and cyber espionage (Mengidis et al., 2019). Each type of cybercrime comprises steps that attackers typically follow to gain access to the desired information. Consequently, protective measures can be implemented for each cyber threat based on their processes.

3. Recent Developments of Cyber Security

In our world of ever-increasing digital interconnectivity, comprehension of the subtleties inherent in these cyber-attack methodologies and the far-reaching consequences they may entail is not a luxury but a necessity. As our lives, economies, and societies continue to migrate into the digital realm, the foundation laid by this comprehensive background study becomes all the more critical (Khan et al., 2020). It is a guide to our understanding of cybersecurity's multifaceted challenges. It underscores the urgency of devising and implementing the strategies and defences vital to safeguarding our digital future (Kaur & Ramkumar, 2022). The inexorable march of progress is upon us, and cybersecurity guardians must remain vigilant, ready to adapt, and fortified with the knowledge and tools to secure the digital frontier (Mehrpooya et al., 2021). The rapid advancement of technology introduces a broad spectrum of risks in the dynamic field of cybersecurity, from the intricacies of artificial intelligence to the extensive network of the Internet of Things. While these new frontiers hold great promise for progress, they also carry inherent uncertainties. The interaction between human nature and technology creates complexity and knowledge gaps in the psychology-tech dance (Kuzlu et al., 2021). Education serves as a beacon, helping individuals navigate the dangerous waters of social engineering. Beyond individual devices, the networked digital environment tangles with complex supply chains, necessitating vulnerability awareness (Mijwil et al., 2023; Rahman et al., 2020).

Cyber security plays an important role in modern Internet of Things (IoT) sectors. The significance of cyber security in the domain of IoT cannot be exaggerated. The convergence of cyber security and the is a crucial junction that requires meticulous consideration because of the profound influence of IoT on diverse businesses (Lee, 2020). With the increasing interconnectivity of gadgets, the potential vulnerability to cyber threats grows at an exponential rate. The dangers encompass a spectrum of risks, including unlawful entry into confidential information, disruption of vital services, and the compromising of entire networks. Considering the wide range of uses for IoT, such as in smart homes, healthcare, industrial processes, and smart cities, the consequences of a security breach can have extensive and serious impacts (Ashraf et al., 2023; Djenna et al., 2021; Jony & Arnob, 2024; Kotenko et al., 2022). In the context of cyberspace, responsibility and attribution are illusive, casting doubt over response operations. Organisational insider threats require a careful balancing act between security, privacy, and trust. Increased security is necessary due to critical infrastructure vulnerabilities, which affect everything from transportation networks to electricity grids. Complexity arises from having to navigate regulatory currents since every industry and area has a different compliance path to follow. Growing cloud computing offers opportunities but also raises concerns about data security, necessitating ongoing changes to shared responsibility models. This investigation reveals cybersecurity's dark corners and emphasises the need for ongoing preparation against nameless enemies (Altulaihan et al., 2022; Ghimire & Rawat, 2022).

4. Methods

This review employs a systematic and comprehensive approach to investigate various aspects of cyber security attacks, aiming to provide valuable insights and identify avenues for further research in this critical domain. This research's methodology is based on a hybrid of concept-context analysis and systematic literature review techniques, with inspiration drawn from existing publications in the field as mentioned by Tranfield et al., (2003) and (Kraus et al., 2020).

This methodology ensures the review process's rigor, transparency, and scientific credibility, setting it apart from traditional narrative reviews (Mulrow, 1994; Oakley, 2002). The methodology adopted in this study aims to rigorously examine the existing literature on cyber security attacks and their implications. This study adheres to the procedures outlined by Kumar et al. (2021) to organize the data. This review will go through three cycles: (1) preparing for the review, (2) performing the review, and (3) reporting the review (discussed in section 4).

4.1. Planning the review

The current study adopts a systematic literature review, employing an inductive reasoning approach to examine cyber security attacks comprehensively. A specific set of well-defined criteria, such as search database, search keywords, and subject areas, is utilized to identify a corpus of relevant scholarly documents, facilitating a structured, integrated, and narrated literature review (Kraus, et al., 2022a).

The criteria and data selection process outlined by Kraus, et al. (2022b) is followed to ensure a robust and comprehensive search. The primary databases used for this review include Web of Science (WoS), Google Scholar, and Springer. WoS was selected because it has a very good reputation as one of the premier databases for scholarly articles and citations, encompassing publications from top-tier journals that are highly relevant for a systematic literature review (Korom, 2019). Google Scholar, renowned for its

accessibility and vast coverage of academic literature across various disciplines, is also utilized to identify valuable sources for this study. And Springer is also a reputable publishing company with a diverse range of academic journals and scientific publications, contributing to the breadth and quality of the literature corpus. Considering the subject matter of cyber security attacks, IEEE Explorer is included as a supplementary database. As an excellent resource for computer science and engineering research, including cybersecurity-related studies, IEEE Explorer offers a valuable collection of papers and conference proceedings that enhance the review's scope (Rzepka & Berger, 2018). The search is restricted to English academic journal articles in select fields: Healthcare Systems, Manufacturing Sectors, Education Systems, Finance Research Areas, Development Sectors, Business, and Management. While intelligence is a topic explored in various disciplines, this study focuses solely on publications within the business and management domain to ensure the selected journals' relevancy and applicability.

In adherence to academic integrity principles, proper attribution and citation practices are followed throughout the study. The review process involves an unbiased and meticulous assessment of the identified literature, leading to the synthesis and interpretation of key findings related to cyber security attacks.

4.2. Performing the review

This section presents how the review has been performed and particularly, a brief description of the systematic review process and article selection at various stages.

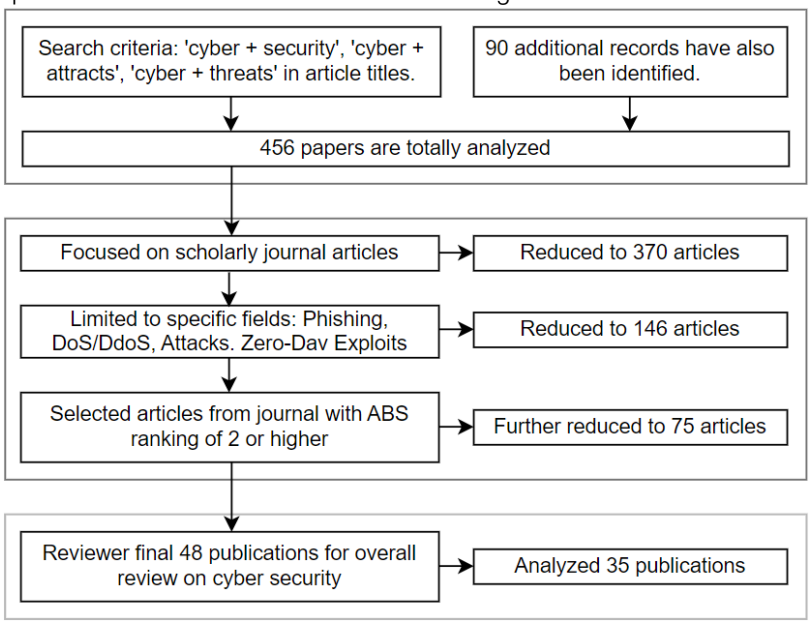

Fig. 1. Flowchart illustrating the systematic review process and article selection at various stages.

In the review process, an initial search utilizing keywords like 'cyber security attacks', 'cyber threats', 'malware', 'phishing', and 'denial of service' will yield a substantial number of articles followed by a focused selection of scholarly journal articles from top-tier academic journals in information security and related fields. The final dataset will be meticulously curated based on a comprehensive review of titles, abstracts, keywords, and content, with inclusion criteria emphasizing articles providing valuable insights into cyber security attacks. These selected articles will be categorized by the type of cyber security attacks, methodologies employed, and impact assessments, allowing for identifying patterns and trends within various attack vectors. Subsequently, key findings will be synthesized and interpreted to comprehensively understand cyber security attacks, their characteristics, and countermeasures, facilitating meaningful conclusions and guiding future research directions.

Fig. 1 illustrates the step-by-step article selection process for a cyber security research study. Starting with 456 articles, it narrowed to 35 high-quality publications after focusing on scholarly sources, specific subfields, journal ranking, and assessing relevance. These 35 articles were chosen for an in-depth analysis of the study.

5. Types of Cyber Attacks

5.1. Malware

Malicious software, or malware, is any program or piece of code that was written with the express purpose of causing harm, compromising security, or exploiting vulnerabilities in computer systems,

networks, or devices. Malicious actors produce and release malware for various reasons, including but not limited to financial gain, data theft, system disruption, espionage, or unlawful access to secret information. It includes numerous harmful programs, each with unique properties and goals (Aslan & Samet, 2020; Bridges, 2008; Or-Meir et al., 2019; Qabalin et al., 2022; Razaulla et al., 2023).

There are many malware assaults, exposing the different techniques hackers employ to compromise computer networks and steal confidential data. Here are some common malware attacks:

- **Viruses**: Viruses are self-replicating malware attached to legitimate files or programs. The replication and dissemination of the virus occurs through the execution of infected files, thereby affecting more files and systems.
- **Worms**: Without attaching to other files, worms can multiply and spread across networks and devices. When spreading, they frequently take advantage of security holes in networks.
- **Trojans**: Trojans, also known as Trojan horses, disguise as legal software but conceal malicious code. Typically, users are duped into executing them, allowing attackers to obtain unauthorized access or perform malicious actions.
- **Ransomware**: Ransomware is malicious software that encrypts a user's data so they can't access it unless the user pays a ransom, typically in cryptocurrency, to unlock the contents. In most cases, paying the ransom is not recommended because doing so provides no assurance that the data may be recovered.
- **Spyware**: Spyware is malicious software that surreptitiously observes and gathers data about a user's actions, encompassing keystrokes, browsing patterns, and login details. The pilfered data is subsequently transmitted to a distant assailant for diverse objectives.
- **Adware**: The ads that adware presents to consumers are often invasive and unwelcome. Though not as dangerous as some malware, it can be annoying and slow down our computer.
- **Rootkits**: Rootkits are malicious software that exhibits stealthy behavior by obtaining elevated privileges on a computer system and concealing its existence, posing detection challenges. They can facilitate Backdoor access, enabling attackers to gain unauthorized entry.

Table 1
Overview of malware types, characteristics, and attack vectors.

Malware Type	Description	Common Characteristics	Common Attack Vectors
Viruses	Self-replicating malware that attaches to legitimate files.	- Replication and spreading - Payload execution upon activation - Damage or data destruction	Email attachments, infected software downloads
Worms	Self-replicating malware that spreads across networks.	- Network propagation - Rapid spreading - Autonomous operation	Network vulnerabilities, infected devices, email attachments
Trojans	Malware disguised as legitimate software.	- Deceptive appearance - Unauthorized access - Remote control	Downloads from malicious websites, email attachments
Ransomware	Malware that encrypts files and demands a ransom.	- Data encryption - Ransom demand - Time-sensitive deadlines	Phishing emails, malicious attachments, exploit kits
Spyware	Stealthy malware that gathers user data.	- Data collection - Keylogging - Data exfiltration	Drive-by downloads, infected email attachments
Adware	Displays unwanted advertisements to users.	- Advertising revenue generation - Intrusive ads - Slows system performance	Bundled with free software, malicious downloads
Rootkits	Malware that hides its presence and provides backdoor access.	- Evasion of detection - Privileged access - Persistent presence	Exploits, social engineering, drive-by downloads
Botnets	Networks of compromised devices controlled by a central server.	- Coordination of attacks - Distributed infrastructure - Amplification attacks	Exploited vulnerabilities, drive-by downloads, infected devices

- **Botnets**: Botnets are collections of compromised gadgets, commonly known as "bots" or "zombies," under a central server's direction. Malicious actors utilize botnets to execute synchronized assaults,

such as distributed denial-of-service (DDoS) attacks or spam campaigns.

Table 1 thoroughly examines multiple dimensions within the realm of malware. It organizes and elucidates diverse categories of malware, delineates their distinctive features, and clarifies the pathways through which they infiltrate computer systems.

5.2. Phishing

Phishing refers to a cyberattack wherein individuals are deceived into divulging sensitive information, such as login passwords, credit card details, or personal data, on the false preteens of interacting with a reliable entity or through deceptive strategies (Aleroud & Zhou, 2017; Kalaharsha & Mehtre, 2021). The name "phishing" is derived from the metaphorical association with the act of "fishing," when passwords and credentials are sought after from users within the realm of the Internet. The name "ph" originates in the practice known as "phone phreaking" a widely utilized technique for exploiting telephone systems throughout the 1970s (Jain & Gupta, 2022). The term "phishing" was initially coined by a collective of cybercriminals operating on the Internet in the year 1996. The hackers used deceptive strategies to obtain the credentials of unsuspecting customers of America Online (AOL), thereby acquiring unauthorized entry into their AOL accounts (Chiew et al., 2018). Phishing attacks have the potential to manifest through a range of communication channels, encompassing electronic mail, online platforms, short message services, and telephonic interactions (Alkhalil et al., 2021; Tandale & Pawar, 2021; Zieni et al., 2023).

Phishing attacks come in various forms, each with its own unique approach and objectives. Here are some common phishing attacks:

- **Email phishing**: Email phishing is a deceptive practice employed by attackers wherein they distribute fraudulent emails that mimic the appearance of genuine communications. These emails are generally designed to create a sense of urgency, compelling recipients to engage with dangerous links or download infected attachments.
- **Spear Phishing**: Spear phishing is a type of phishing that involves tailoring communications to target a specific individual or organization. To enhance the persuasiveness of their phishing attempt, individuals collect pertinent information about the target.
- **Whaling**: Similar to spear phishing, it is a cyber-attack strategy that focuses explicitly on prominent individuals, such as executives or CEOs, to illicitly obtain confidential corporate information.
- **Vishing**: Short for "voice phishing," vishing involves using phone calls to deceive victims into disclosing sensitive information or performing actions like transferring funds.
- **Smishing**: Smishing, or "SMS phishing," uses text messages to deliver malicious links or requests for personal information.

Table 2
Overview of phishing types, characteristics, and attack vectors.

Phishing Types	Characteristics	Common Attack Patterns
Email Phishing	• Involves fraudulent emails resembling legitimate sources. • Often employs urgent or enticing messages.	• Sending deceptive emails with malicious links or attachments. • Impersonating trusted entities.
Spear Phishing	• A targeted form of phishing with personalized messages. • Leverages information about the victim for credibility.	• Crafting tailored messages based on the victim's profile. • Gathering intelligence for convincing impersonation.
Whaling	• Focuses on high-profile individuals, such as executives. • Aims to steal sensitive corporate data.	• Targeting top-level executives. • Exploiting their access to valuable corporate information.
Vishing	• Short for "voice phishing" using phone calls. • Deceives victims into revealing information or taking action.	• Making phone calls with deceptive intentions. • Convincing victims to provide sensitive data or carry out unauthorized actions.
Smishing	• Also known as "SMS phishing" using text messages. • Delivers malicious links or requests for personal info.	• Sending text messages with fraudulent links. • Requesting personal information via text messages.

Table 2 provides a succinct and organized overview of diverse phishing strategies, distinctive attributes, and the attack vectors utilized by malevolent individuals. The presented table provides a significant resource for comprehending the multifaceted nature of phishing attempts, imparting knowledge on how

cybercriminals manipulate human psychology and exploit vulnerabilities inside digital communication channels.

5.3. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks

Denial of Service or DoS, and Distributed Denial of Service, or DDoS attacks, are malicious tactics designed to disrupt the availability and functionality of computer systems, websites, or networks. In a DoS attack, a single source overwhelms a target server or network with excessive traffic, rendering it incapable of serving legitimate user requests. On the other hand, DDoS attacks involve multiple distributed sources, often compromised computers forming a botnet, collectively bombarding the target. These attacks exploit vulnerabilities in network protocols or server resources, such as bandwidth or processing power, leading to service degradation or complete unavailability. Their motivations range from hacktivism and revenge to financial gain or diversionary tactics, making them a persistent and challenging cybersecurity concern. Mitigation solutions encompass various measures, such as traffic filtering, rate restriction, and the utilization of specialized Distributed Denial of Service (DDoS) protection services aimed at absorbing and mitigating the adverse effects caused by such attacks (Gniewkowski, 2020; Peng et al., 2007; Prasad et al., 2014).

Following is a discussion of cyber dangers and vulnerabilities, emphasizing different varieties of DoS and DDoS attacks. We will examine the unique features and techniques of these destabilizing attacks, focusing on the harm they cause to digital services and the methods used to counteract them:

- Traditional DoS: In a conventional DoS attack, a single attacker or a small group of attackers flood a target with traffic, often using botnets or multiple systems under their control.
- DDoS Attack: A Distributed Denial of Service (DDoS) attack involves a coordinated effort from multiple compromised devices or systems (often part of a botnet) to overwhelm the target. This makes DDoS attacks more powerful and challenging to mitigate.

5.4. Zero-day exploits

A zero-day attack is a type of cyber assault that exploits an exposure that hasn't been publicly disclosed. These attacks are exceptionally challenging to defend against because, as long as the exposure remains undisclosed, the affected software cannot be patched, and traditional antivirus solutions cannot identify the attack using signature-based scanning (Blaise et al., 2020). In other words, it exploits a weakness in software before the vendor has had the opportunity to develop and release a patch (software update) to fix it. For cybercriminals, unpatched susceptibilities in widely used software applications like Microsoft Office or Adobe Flash provide them with an open door to target any entity they desire, ranging from large Fortune 500 corporations to countless individual PCs worldwide. This is why the market value of a new susceptibility varies widely, ranging from $5,000 to $250,000 (Bilge & Dumitras, 2012; Miller, 2007). Zero-day vulnerabilities are typically associated with targeted attacks, as indicated by post-incident analyses linking these vulnerabilities to zero-day attacks (Symantec, 2014). Previous research has concentrated on the entire vulnerability exposure period, encompassing the time until all vulnerable systems are patched and covering attacks occurring after the vulnerability disclosure (Schneier, 2000). Zero-day exploits are of great interest to cybercriminals and hackers sponsored by governments due to their ability to exploit vulnerabilities in systems without being detected or mitigated immediately.

The discussion below covers various prevalent categories of zero-day exploits, which pose a significant challenge in the constantly evolving digital threat environment.

- Zero-Day Vulnerability: This refers to the specific security flaw or weakness in software or hardware that is unknown and unpatched. Attackers discover and exploit these vulnerabilities.
- Zero-Day Attack: The actual exploitation of the zero-day vulnerability constitutes a zero-day attack. Attackers create or obtain exploit code that exploits the vulnerability to compromise systems.

5.5. Man-in-the-Middle (MITM) attacks

MITM attack is a cyber threat where a malicious third party covertly gains control over the transmission channel connecting two or more endpoints. The concept of "Man-In-The-Middle" is derived from a basketball comparison, wherein two players endeavour to exchange the ball while a third player intervenes in an attempt to intercept it (Nayak & Samaddar, 2010). Alternatively, MITM attacks are sometimes referred to as "bucket brigade attacks" or "fire brigade attacks" (Haataja & Hypponen, 2008; Nayak & Samaddar, 2010). A typical MITM scenario has two victims or endpoints and an attacker. The attacker infiltrates the communication channel between these endpoints, enabling them to manipulate the exchanged messages (Conti et al., 2016; Ornaghi & Valleri, 2003). If attackers can compromise encryption keys or certificates, MITM attacks can manifest in various contexts, such as public Wi-Fi networks, corporate environments, and encrypted communication channels. Protection against MITM attacks necessitates the implementation of encryption protocols like HTTPS and robust authentication methods (Ollmann, 2007). Additionally, users

should exercise caution when connecting to unfamiliar or unsecured networks.

Man-in-the-Middle (MitM) attacks consist of a variety of tactics and strategies used by malicious individuals to intercept and control the communication between two parties. Here, we'll explore some common typical forms of MitM attacks:

- Spoofing-based MITM: This attack involves an intruder using spoofing techniques to intercept legitimate communication between two hosts, thereby seizing control of the transmitted data without the hosts' knowledge.
- SSL/TLS MITM: This active network interception involves the attacker's insertion into the communication channel, establishing a connection between two parties, often a victim's web browser and a web server. The assailant initiates two distinct SSL connections with the targets and functions as an intermediate, thereby concealing their existence from both parties involved. The arrangement above facilitates the attacker's interception of all transmitted communications, who can then selectively modify the data being delivered.
- BGP MITM: This attack leverages IP hijacking, with the attacker redirecting stolen traffic to reach its intended destination. Consequently, the traffic passes through the attacker's Autonomous System (AS), which can be manipulated.
- False Base Station-based (FBS-based) MITM: In this attack, a third party compels the victim to establish a connection with a counterfeit Base Transceiver Station (BTS). Subsequently, the attacker utilizes this connection to exploit the victim's traffic, exerting control over the data transmission process.

Table 3
Overview of MITM types, characteristics, and attack vectors.

MITM Types	Characteristics	Common Attack Vectors
Spoofing-based MITM	Intercepting legitimate communication.	ARP spoofing, DNS spoofing, IP spoofing, MAC spoofing.
SSL/TLS MITM	• Dynamic network interception. • Relay between sufferers. • Undetectable presence.	SSL stripping, HTTPS downgrade attacks, Rogue SSL certificates.
BGP MITM	• Exploits IP hijacking. • Traffic redirection. • Manipulation within attacker's AS.	BGP route hijacking, Prefix subordination, AS path poisoning, Prefix filtering attacks.
FBS-based MITM	• Forces victim to connect to a fake BTS. • Manipulates victim's traffic through the fake BTS. • Control over data transmission.	Impersonation of legitimate cell tower, IMSI catchers, LTE interceptors, Stingray devices.

Table 3 provides an in-depth analysis of MITM assaults, exploring their many varieties, elaborating on their distinctive features, and detailing the methods criminals employ to monitor and manipulate communications between unsuspecting victims. It's an organized resource for learning about man-in-the-middle attacks and the methods used by hackers to exploit flaws in digital communication.

5.6. SQL injection attacks

Identifying SQL injection vulnerabilities has been acknowledged as a significant peril to web applications. Web applications susceptible to SQL injection can grant attackers unrestricted access to the underlying databases (Halfond et al., 2006; Nasereddin et al., 2021; Sadeghian et al., 2013; Singh et al., 2016). The storage of sensitive user or consumer data in these databases often results in substantial consequences in the event of security breaches (Abdullayev & Chauhan, 2023; Clarke, 2009). The ramifications include identity theft, the divulgence of personal data, and the commission of deceitful activities. SQL injection is a code-injection attack wherein user-supplied data is incorporated into a SQL query, resulting in the user's input being interpreted as SQL code. An attacker can leverage the vulnerabilities to execute SQL statements on the database. In a study conducted by Fredj et al. (2021), SQL injection attacks manifest in various forms, targeting distinct facets of SQL database queries. Here are some prevalent SQL injection attack types:

- Traditional SQL Injection: In this attack variant, malicious SQL code infiltrates user inputs, often found in web forms. This illicit code manipulates SQL queries, potentially granting unauthorized access, data extraction, or even tampering with the database.
- Blind SQL Injection: Blind SQL injection exploits vulnerabilities without directly observing the attack's outcomes. Attackers inject harmful code to scrutinize the database's response, often utilizing Boolean-

based or time-based methods to confirm code execution.

- **Time-Based Blind SQL Injection**: Time-based blind SQL injection introduces delays within SQL queries, indirectly validating the success of injected code. Attackers gauge conditions or injections through response delays.
- **Error-Based SQL Injection**: Error-based SQL injection involves injecting code to compel the database to generate errors. These errors frequently disclose valuable database structural details, facilitating further exploitation.
- **Union-Based SQL Injection**: Union-based SQL injection capitalizes on the SQL UNION operator to merge data from multiple database tables. Attackers insert code featuring a UNION statement, allowing data extraction from additional tables.

Table 4
Overview of SQL injection types, characteristics, and attack vectors.

SQL Injection Types	Characteristics	Common Attack Patterns
Traditional SQL Injection	• Infiltrates user inputs, often in web forms. • Manipulates SQL queries. • Can grant unauthorized access, data extraction, or tampering with the database.	• Injecting malicious SQL code into input fields. • Altering input to manipulate queries. • Extracting data or modifying the database.
Blind SQL Injection	• Exploits vulnerabilities without observing outcomes. • Relies on probing the database's response. • Often uses Boolean or time-based techniques.	• Injecting malicious code to test responses. • Boolean-based queries. • Time-based delays to confirm code execution.
Time-Based Blind SQL Injection	• Introduces delays in SQL queries. • Indirectly validates injected code success. • Relies on response delays.	• Injecting code with time delays. • Monitoring response times.
Error-Based SQL Injection	• Injects code to force database errors. • Reveals database structural details. • Facilitates further exploitation.	• Injecting code to generate errors. • Analyzing error messages for information.
Union-Based SQL Injection	• Utilizes SQL UNION operator to merge data from multiple tables. • Allows data extraction from additional tables.	• Injecting code with UNION statements. • Extracting data from multiple tables.
Out-of-Band SQL Injection	• Exfiltrates data through a separate communication channel. • May use DNS or alternative protocols for data transfer.	• Redirecting data to external channels. • Utilizing DNS or alternative protocols for data retrieval.
Second-Order SQL Injection	• Injects data initially without immediate impact. • Exploits injected data in subsequent queries. • Creates exploitation opportunities.	• Injecting data without immediate consequences. • Awaiting subsequent query use for exploitation.
Content-Based SQL Injection	• Manipulates queries based on retrieved content. • Alters application behavior. • Can lead to data theft or unauthorized actions.	• Modifying queries based on retrieved data. • Altering application behavior through input.
Boolean-Based SQL Injection	• Inserts code based on true or false conditions. • Infers information from application responses. • Determines code execution.	• Crafting code based on Boolean conditions. • Analyzing responses for true or false outcomes.
Time-Based Blind SQL Injection	• Introduces delays in SQL queries. • Validates success via response times. • Facilitates data extraction.	Monitoring response times for confirmation.

- **Out-of-Band SQL Injection**: Data is exfiltrated through a distinct communication channel in this variation. Attackers may utilize DNS or alternative protocols to transfer data from the database to a location under their control.

- Second-Order SQL Injection: Second-order SQL injection commences with the injection of malicious code that initially does not affect the application. However, the injected data is subsequently used in a query, creating opportunities for exploitation.
- Content-Based SQL Injection: Attackers manipulate queries contingent upon content retrieved from the database, thus altering the application's behaviour. Content-based SQL injection poses severe risks, potentially leading to data theft or unauthorized actions.
- Boolean-Based SQL Injection: In Boolean-based SQL injection, attackers insert code reliant on true or false conditions. They deduce information by assessing the application's response to determine code execution.
- Time-Based Blind SQL Injection: Time-based blind SQL injection introduces delays in SQL queries, relying on the application's response time to validate successful injections. This technique indirectly facilitates data extraction from the database.

Table 4 presents the characteristics, attack vectors, and a comprehensive examination of SQL injection attacks. This structured reference delineates the various forms of SQL injection, their defining characteristics, and the attack vectors employed by malicious actors to exploit vulnerabilities in database systems. Fig. 2. illustrates the hierarchy of common cybersecurity threats.

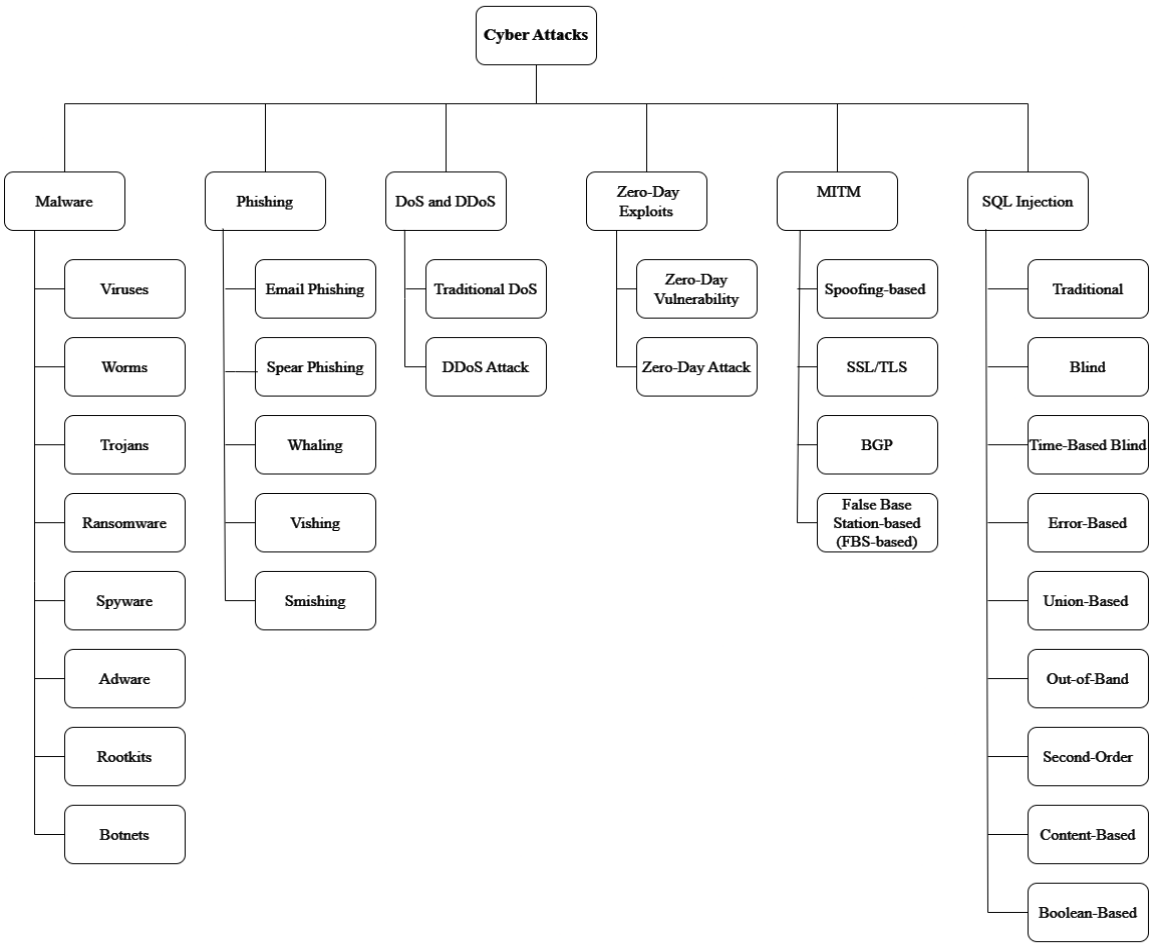

Fig. 2. Hierarchy of common cybersecurity threats.

6. Results and Discussion

Cybersecurity assumes an indispensable role in our contemporary digital landscape, given the persistent and continually evolving onslaught against computer systems, networks, and data storage facilities. It stands as a paramount concern for entities ranging from companies and governments to individuals, particularly as the digital revolution pervades every facet of society. Cyber threats manifest in diverse and deceptive forms, such as phishing assaults, malware infiltrations, DOS and DDoS attacks, Zero-Day Exploits, Man-in-the-Middle attacks, and SQL Injection Attacks. Each potential entry point poses distinct challenges. In contrast, malware, a form of software meticulously crafted to clandestinely breach computer systems

with the intent of extracting data, underscores the stealthy nature of these threats. Simultaneously, phishing attempts exploit human psychology and trust to trick individuals into revealing sensitive information. DDoS attacks, capable of wreaking havoc on businesses, have the potential to damage entire networks, rendering essential services unavailable. Effectively mitigating cybercrime necessitates a comprehensive understanding of the motivations and methodologies employed by cybercriminals, who engage in these attacks for various purposes, including financial gain, data theft, political espionage, and hacktivism.

Fig. 2. shows the hierarchical structure which serves as a visual guide to the various cyber threats that has been covered in this paper. As we can see, the intricate interdependencies and associations across diverse forms of attacks, facilitating a holistic comprehension of the dynamic cybersecurity environment. With the rapid progression of technology, individuals, businesses, and governments must be aware of and adopt proactive security measures due to the ongoing development of new strategies and the exploitation of weaknesses by cyber criminals.

Table 5 presents an overview of various cyberattack types and their characteristics with key examples of each attack type.

Table 5

An overview of various cyberattack types and their characteristics.

Attack Type	Description	Common Characteristics	Key Examples
Phishing	Deceptive tactics to trick users into revealing information.	Spoofing legitimate entities, Use of urgency and fear, Fake login pages, Credential theft.	Email phishing, Spear phishing, Smishing.
DoS/DDoS Attacks	Overwhelming target systems or networks to disrupt service.	Volume-based attacks, Protocol-based attacks, Application layer attacks, Amplification attacks, Exploiting vulnerabilities.	SYN Flood, HTTP Flood, DNS Amplification.
Zero-Day Exploits	Exploiting undiscovered vulnerabilities for unauthorized access.	Stealthy attacks, Targeting high-value entities, APTs and espionage, financial gain.	Stuxnet, WannaCry, Heartbleed.
Man-in-the-Middle (MitM)	Intercepting and manipulating communication between parties.	Eavesdropping, Data manipulation, Session hijacking, SSL Stripping, ARP Spoofing.	ARP Poisoning, SSL Stripping, DNS Spoofing.
SQL Injection Attacks	Injecting malicious SQL code into web application inputs.	SQL payload injection, Error-based SQLi, Blind SQLi (Boolean and time-based), Union-based SQLi.	Classic SQL Injection, Blind SQL Injection.
Malware	Broad term for malicious software compromising systems.	Various types (viruses, worms, Trojans, ransomware, spyware, etc.), Harmful intent, Data theft, System disruption.	Conficker, WannaCry, NotPetya, Zeus.

As the digital world undergoes continuous growth and transformation, the significance of robust cybersecurity measures intensifies. The global reach and impact of cybercrime underscore the imperative to implement thorough and pre-emptive cybersecurity strategies. This discourse underscores the critical necessity of developing and deploying tactics and defences to safeguard our digital future. In an era where daily life, businesses, and communities increasingly rely on digital infrastructure, cybersecurity stands as the bulwark against the ever-changing threats accompanying technological advances. Cybersecurity professionals must maintain perpetual vigilance, flexibility, and preparedness to protect the digital frontier from the inevitable progress of technology.

Table 6 presents a comprehensive matrix to visualize the common patterns have among the cyberattacks.

7. Conclusions

In today's digital era, a detailed examination of cybersecurity attacks underscores the immediate need for robust defences against harmful threats. With growing interconnectedness and reliance on digital infrastructures, combating hackers and malicious actors has become more critical than ever. In light of the increasing interconnectedness and dependence on digital systems, the significance of the ongoing struggle against hackers and hostile actors has reached unprecedented levels. The growth and sophistication of cybersecurity threats, encompassing techniques such as phishing, malware, DoS, and DDoS assaults, persistently provide significant challenges. Gaining insight into the underlying motivations behind cyber-attacks, encompassing objectives such as financial profit, data exfiltration, espionage, and hacktivism, is paramount

in formulating efficacious strategies for countering such threats. The repercussions of these attacks transcend particular targets, exerting a global influence on companies and individuals. The global repercussions of cyber-attacks underscore the need for proactive and comprehensive cybersecurity measures. As society progresses in the digital age, the significance of cybersecurity as a safeguard against ever-changing risks grows.

Table 6
An overview of cyberattack common pattern comparison matrix.

Pattern / Attack Type	Stealthy	Target High-Value Entities	Financial Gain	Data Theft	System Disruption	Exploits Vulnerabilities	Evasion Techniques	Coordination
Malware	✓	✓	✓	✓	✓	✓	✓	✓
DoS/DDoS Attacks					✓	✓	✓	X
Zero-Day Exploits	✓	✓	✓	✓		✓	✓	X
Man-in-the-Middle (MitM)	✓	X	X	X	X	X	✓	X
SQL Injection Attacks	✓	X	X	X	X	X	✓	X
Phishing	X	X	✓	✓	X	X	X	X

(Note: Here the '✓' means that these cyberattack have common pattern which have been found in the article that we have reviewed and 'X' means those attacks doesn't have the common property).

The lessons derived from the diverse cybersecurity threats underscore the significance of being prepared, vigilant, and continuously adapting security tactics. Future cybersecurity research should delve into integrating emerging technologies like artificial intelligence and machine learning for heightened threat detection. Understanding human-centric aspects, such as user behaviour, and formulating effective cybersecurity education strategies is crucial. To protect our digital future, we must work together and remain steadfastly committed to proactively counteracting the ever-evolving tactics used by cybercriminals.

8. References

Abdullayev, V., & Chauhan, A. S. (2023). SQL Injection Attack: Quick View. *Mesopotamian Journal of Cyber Security.*, *2023*, 30–34.

Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber Threat Intelligence – Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371–379. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Alghamdi, M. I. (2021). WITHDRAWN: Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.04.093

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. *Electronics*, *11*, 3330.

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. Bin, & Nosheen, S. (2023). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2677–2690.

Aslan, Ö., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. *IEEE Access*, *8*, 6249–6271. https://doi.org/10.1109/ACCESS.2019.2963724

Bilge, L., & Dumitras, T. (2012). Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World. *CCS '12: Proceedings of the 2012 ACM Conference on Computer and Communications Security*, 833–844.

Blaise, A., Bouet, M., Conan, V., & Secci, S. (2020). Detection of zero-day attacks: An unsupervised port-based approach. *Computer Networks*, *180*, 107391. https://doi.org/10.1016/j.comnet.2020.107391

Bridges, L. (2008). The changing face of malware. *Network Security*, *2008*(1), 17–20.
Brown, S., Gommers, J., & Serrano, O. (2015). From Cyber Security Information Sharing to Threat Management. *WISCS '15: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, 43–49.
Cavelty, M. D. (2010). Cyberwar: Concept, Status Quo, and Limitations. *CSS Analyses in Security Policy*, *71*. https://doi.org/https://doi.org/10.3929/ethz-a-006122108
Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1–20. https://doi.org/10.1016/j.eswa.2018.03.050
Clarke, J. (2009). *SQL Injection Attacks and Defense*. Elsevier. https://doi.org/10.1016/B978-1-59-749963-7.00001-3
Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man In The Middle Attacks. *IEEE Communications Surveys & Tutorials*, *18*(3), 2027–2051.
Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Applied Sciences*, *11*(10), 4580.
Fredj, O. Ben, Cheikhrouhou, O., Krichen, M., Hamam, H., & Derhab, A. (2021). An OWASP Top Ten Driven Survey on Web Application Protection Methods. *International Conference on Risks and Security of Internet and Systems*, 235–252. https://doi.org/10.1007/978-3-030-68887-5
Furnell, S., & Shah, J. N. (2020). Home working and cyber security – an outbreak of unpreparedness? *Computer Fraud & Security*, *2020*(8), 6–12. https://doi.org/10.1016/S1361-3723(20)30084-1
Ghelani, D. (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology*, *3*(6), 12–19. https://doi.org/10.11648/j.XXXX.2022XXXX.XX
Ghimire, B., & Rawat, D. B. (2022). Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things. *IEEE Internet of Things Journal*, *9*(11), 8229–8249. https://doi.org/10.1109/JIOT.2022.3150363
Gniewkowski, M. (2020). An Overview of DoS and DDoS Attack Detection Techniques. *International Conference on Dependability and Complex Systems*.
Haataja, K. M. J., & Hypponen, K. (2008). Man-In-The-Middle attacks on bluetooth: a comparative analysis, a novel attack, and countermeasures. *2008 3rd International Symposium on Communications, Control and Signal Processing*, 1096–1102.
Halfond, W. G. J., Viegas, J., & Orso, A. (2006). *A Classification of SQL Injection Attacks and Countermeasures*.
Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, *95*, 101827. https://doi.org/10.1016/j.cose.2020.101827
Hawamleh, A. M. AL, Alorfi, A. S., Al-Gasawneh, J. A., & Al-Rawashdeh, G. (2020). Cyber Security and Ethical Hacking: The Importance of Protecting User Data. *Solid State Technology*, *63*(5).
Hayzelden, A. L. G., Bigham, J., Wooldridge, M., & Cuthbert, L. G. (1999). Future Communication Networks using Software Agents. In *Software Agents for Future Communication Systems* (p. 1999).
Jain, A. K., & Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, *16*(400), 527–565. https://doi.org/10.1080/17517575.2021.1896786
Jony, A. I., & Arnob, A. K. B. (2024). A long short-term memory based approach fordetecting cyber attacks in IoT using CIC-IoT2023dataset. *Journal of Edge Computing*.
Kalaharsha, P., & Mehtre, B. M. (2021). *Detecting Phishing Sites - An Overview*.
Karbasi, A., & Farhadi, A. (2021). A cyber-physical system for building automation and control based on a distributed MPC with an efficient method for communication. *European Journal of Control*, *61*, 151–170. https://doi.org/10.1016/j.ejcon.2021.04.008
Kaur, J., & Ramkumar, K. . R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University - Computer and Information Sciences*, *34*(8), 5766–5781. https://doi.org/10.1016/j.jksuci.2021.01.018
Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis and Prevention*, *148*, 105837. https://doi.org/10.1016/j.aap.2020.105837
Korom, P. (2019). A bibliometric visualization of the economics and sociology of wealth inequality: a world apart? *Scientometrics*, *118*, 849–868. https://doi.org/10.1007/s11192-018-03000-z

Kotenko, I., Izrailov, K., & Buinevich, M. (2022). Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches. *Sensors*, *22*(4), 1335.
Kraus, S., Breier, M., & Dasí-Rodríguez, S. (2020). The art of crafting a systematic literature review in entrepreneurship research. *International Entrepreneurship and Management Journal*, *16*, 1023–1042.
Kraus, S., Breier, M., Lim, W. M., Dabić, M., Kumar, S., Kanbach, D., Mukherjee, D., Corvello, V., Piñeiro-Chousa, J., Liguori, E., Palacios-Marqués, D., Schiavone, F., Ferraris, A., Fernandes, C., & Ferreira, J. J. (2022). Literature reviews as independent studies: guidelines for academic practice. *Review of Managerial Science*, *16*, 2577–2595.
Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. *International Journal of Information Management Volume*, *63*, 102466. https://doi.org/10.1016/j.ijinfomgt.2021.102466
Kumar, S., Kar, A. K., & Ilavarasan, P. V. (2021). Applications of text mining in services management: A systematic literature review. *International Journal of Information Management Data Insights*, *1*(1), 100008. https://doi.org/10.1016/j.jjimei.2021.100008
Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, *1*(7). https://doi.org/10.1007/s43926-020-00001-4
Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, *12*(9), 157.
Liu, X., Zhang, J., Zhu, P., Tan, Q., & Yin, W. (2021). Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. *Computers & Security*, *102*, 102138. https://doi.org/10.1016/j.cose.2020.102138
Ma, L., Zhang, Y., Yang, C., & Zhou, L. (2021). Security control for two-time-scale cyber physical systems with multiple transmission channels under DoS attacks: The input-to-state stability. *Journal of the Franklin Institute*, *358*(12), 6309–6325. https://doi.org/10.1016/j.jfranklin.2021.05.017
McCarthy, A., Ghadafi, E., Andriotis, P., & Legg, P. (2022). Functionality-Preserving Adversarial Machine Learning for Robust Classification in Cybersecurity and Intrusion Detection Domains: A Survey. *Journal of Cybersecurity and Privacy*, *2*(1), 154–190.
McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*.
Mehrpooya, M., Ghadimi, N., Marefati, M., & Ghorbanian, S. A. (2021). Numerical investigation of a new combined energy system includes parabolic dish solar collector, Stirling engine and thermoelectric device. *International Journal of Energy Research*, 1–20. https://doi.org/10.1002/er.6891
Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2019). *Blockchain and AI for the Next Generation Energy Grids: Cybersecurity Challenges and Opportunities*. *43*(1), 21–33.
Mijwil, M. M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian Journal of Cyber Security*, 57–63.
Miller, C. (2007). *The Legitimate Vulnerability Market: The Secretive World of 0-Day Exploit Sales*. Independent Security Evaluators. https://www.ise.io/wp-content/uploads/2019/11/cmiller_weis2007.pdf
Muckin, M., Fitch, S. C., & Lockheed Martin Corporation. (2019). *A Threat-Driven Approach to Cyber Security: Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization*.
Mulrow, C. D. (1994). Rationale for systematic reviews. *BMJ*, *309*, 597–599.
Nasereddin, M., Khamaiseh, A. Al, Qasaimeh, M., & Qassas, R. Al. (2021). A systematic review of detection and prevention techniques of SQL injection attacks. *Information Security Journal: A Global Perspective*, *32*(4), 252–265. https://doi.org/10.1080/19393555.2021.1995537
Nayak, G. N., & Samaddar, S. G. (2010). Different flavours of Man-In-The-Middle attack, consequences and feasible solutions. : *: 2010 3rd International Conference on Computer Science and Information Technology*, 491–495.
Oakley, A. (2002). Social Science and Evidence-based Everything: the case of education. *Educational Review*, *54*(3). https://doi.org/10.1080/0013191022000016329
Ollmann, G. (2007). *The Phishing Guide: Understanding & Preventing Phishing Attacks*.
Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. *ACM Computing Surveys*, *52*(5). https://doi.org/10.1145/3329786
Ornaghi, A., & Valleri, M. (2003). Man in the middle Man in the middle attacks. *Blackhat Conference*.
Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys*, *39*(1), 3–es.

https://doi.org/10.1145/1216370.1216373
Prasad, K. M., Reddy, A. R. M., & Rao, K. V. (2014). DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms - A Survey. *Global Journal of Computer Science and Technology*, *14*(7), 15–32.
Qabalin, M. K., Naser, M., & Alkasassbeh, M. (2022). Android Spyware Detection Using Machine Learning: A Novel Dataset. *Sensors*, *22*(15), 5765.
Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393
Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B. C. M., & Assi, C. (2023). The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. *IEEE Access*, *11*, 40698–40723. https://doi.org/10.1109/ACCESS.2023.3268535
Rzepka, C., & Berger, B. (2018). User Interaction with AI-enabled Systems: A Systematic Review of IS Research. *Thirty Ninth International Conference on Information Systems*.
Sadeghian, A., Zamani, M., & Abdullah, S. M. (2013). A Taxonomy of SQL Injection Attacks. *2013 International Conference on Informatics and Creative Multimedia*, 269–273. https://doi.org/10.1109/ICICM.2013.53
Schlette, D., Böhm, F., Caselli, M., & Pernul, G. (2021). Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, *20*, 21–38. https://doi.org/10.1007/s10207-020-00490-y
Schneier, B. (2000). *Crypto-Gram*. https://www.schneier.com/crypto-gram/archives/2000/0915.html
Singh, N., Dayal, M., Raw, R. S., & Kumar, S. (2016). SQL injection: Types, methodology, attack queries and prevention. *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*.
Symantec. (2014). *Internet Security Threat Report 2014* (Vol. 19, Issue April).
Tandale, K. D., & Pawar, S. N. (2021). Different Types of Phishing Attacks and Detection Techniques: A Review. *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*.
Thomson, J. R. (2015). *High integrity systems and safety management in hazardous industries*.
Tranfield, D., Denyer, D., & Palminder Smart. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, *14*, 207–222.
Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39.
Zieni, R., Massari, L., & Calzarossa, M. C. (2023). Phishing or Not Phishing? A Survey on the Detection of Phishing Websites. *IEEE Access*, *11*, 18499–18519. https://doi.org/10.1109/ACCESS.2023.3247135