Global Mainstream Journal of Innovation, Engineering & Emerging Technology

Copyright © The Author(s)
Vol. 03, No. 04, August, 2024
e-ISSN:2998-3967
Page No: 42-57

COMMON CYBERSECURITY VULNERABILITIES: SOFTWARE BUGS, WEAK PASSWORDS, MISCONFIGURATIONS, SOCIAL ENGINEERING

Mahmudul Hasan
https://orcid.org/0009-0006-4030-3243
Graduate Researcher, Master of Science in Management Information Systems, College of Business, Lamar University, Texas, USA
Corresponding Author: mahmudulshojan601@gmail.com

Farhana Zaman Rozony
https://orcid.org/0009-0000-0894-2455
Graduate Researcher, Master of Science in Management Information Systems, College of Business, Lamar University, Texas, USA

Md Kamruzzaman
https://orcid.org/0009-0005-4354-3966
PhD Candidate, Faculty Of Management, Multimedia University, Cyberjaya, Malaysia

Md Kazi Shahab Uddin
https://orcid.org/0009-0000-3209-6818
Master's of Science in Information Technology, Washington University of Science and Technology, Virginia, USA

Keywords

Cybersecurity
Software Bugs
Weak Passwords
Misconfigurations
Social Engineering
Vulnerabilities
Information Security

Article Information

Received: *04 July, 2024*
Accepted: *19 August, 2024*
Published: *20 August,2024*

Doi: 10.62304/jieet.v3i4.193

ABSTRACT

This systematic review examines the most significant cybersecurity vulnerabilities, employing the PRISMA methodology to analyze findings from a comprehensive selection of 150 recent research articles. The study identifies and explores key vulnerabilities, including phishing, compromised credentials, poor encryption, misconfigurations, malicious insiders, ransomware, and exploited trust relationships. The findings highlight the persistent prevalence of phishing and compromised credentials, driven by evolving attacker tactics and the increasing complexity of remote work environments. Technical vulnerabilities such as inadequate encryption and misconfigurations remain critical issues, emphasizing the need for stringent security protocols and continuous monitoring. Malicious insiders continue to pose substantial risks, necessitating robust access controls and comprehensive employee education. The review also underscores the growing sophistication of ransomware attacks, particularly those employing double extortion tactics, and the significant threat posed by compromised trust relationships between organizations. The study concludes that a holistic approach, integrating advanced technical defenses with human-centric strategies, is essential for enhancing cybersecurity resilience and protecting sensitive information in an ever-evolving digital landscape.

1 INTRODUCTION

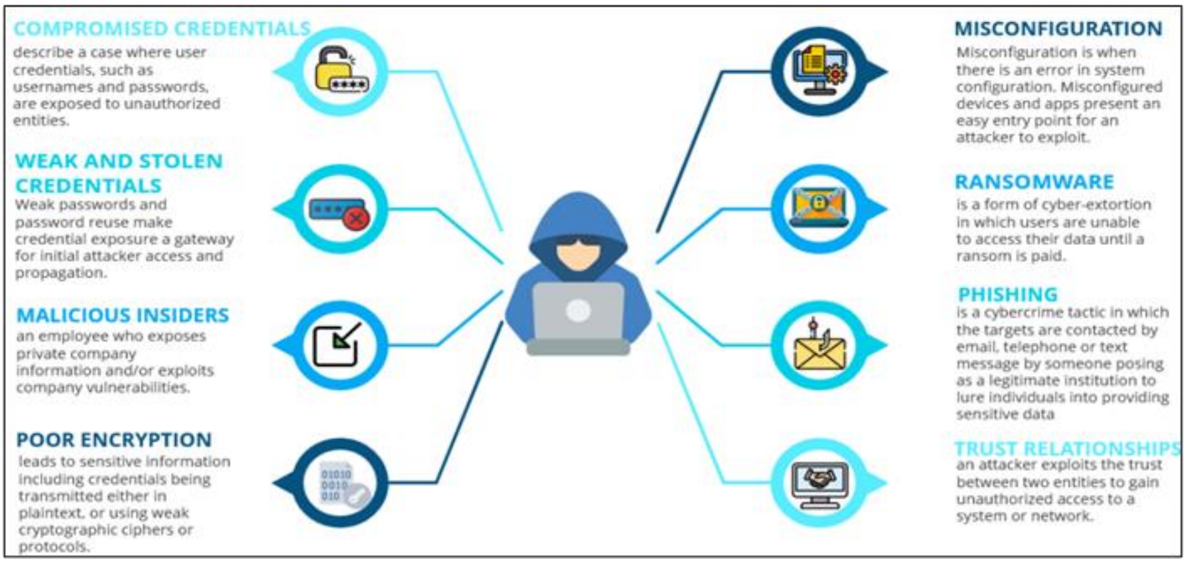
In today's digital landscape, cybersecurity has become a paramount concern for organizations spanning various industries (Yaacoub et al., 2021). The exponential technological growth has undoubtedly offered substantial advantages, streamlining operations and enhancing productivity. However, this technological proliferation has simultaneously unveiled a plethora of vulnerabilities, providing opportunities for malicious actors to exploit these weaknesses (Younes, 2016). As cyber threats evolve in complexity and frequency, it becomes imperative for organizations to identify and understand the nature of these vulnerabilities to safeguard their information assets effectively (Tripathi & Hubballi, 2018). Furthermore, one of the most prevalent cybersecurity vulnerabilities is software bugs. These bugs, often resulting from coding errors, can create significant security gaps that attackers can exploit. ElSawy et al. (2013) highlight that even minor software bugs can lead to significant security breaches if not promptly identified and rectified. Software bugs are a testament to the challenges faced in software development, where the pressure to deliver new features quickly can sometimes overshadow the importance of rigorous testing and quality assurance (Sivathanu et al., 2005; Younus et al., 2024). Software developers and companies continuously strive to find and fix these bugs through various testing methods, yet the sheer complexity of modern software often means that some bugs remain undiscovered until they are exploited. The consequences of such exploits can be severe, ranging from data breaches to system shutdowns, highlighting the critical need for improved coding practices and comprehensive testing protocols (Lun et al., 2019).

Weak passwords constitute another significant vulnerability in cybersecurity. Despite widespread awareness campaigns and the availability of advanced authentication technologies, many users continue to choose easily guessable passwords or reuse the same passwords across multiple platforms (Pan et al., 2011; Younus et al., 2024). Studies indicate that weak passwords are a primary vector for unauthorized access, enabling attackers to compromise systems relatively easily. This ongoing issue points to a broader problem of user behavior and the difficulty in changing it (Amin et al., 2024; Enoch et al., 2018). Users often prioritize convenience over security, opting for simple passwords that are easy to remember rather than secure ones that are hard to crack. Organizations have tried to combat this by enforcing more robust password policies, implementing multi-factor authentication, and educating users about the risks of weak passwords. However, the persistence of this vulnerability suggests that more innovative solutions are needed to address the human factor in cybersecurity (Ramaki et al., 2018).

Misconfigurations, particularly in cloud environments, pose severe risks to cybersecurity. As organizations increasingly migrate to cloud services, the potential for misconfigurations has escalated, leading to unintended data exposures and breaches (Conti et al., 2016). These misconfigurations often stem from a lack of understanding of cloud security settings or the reliance on default configurations, which may not be secure (Hossen et al., 2024; Ramaki et al., 2018). Research has shown that many data breaches in recent years can be attributed to misconfigured cloud resources, highlighting the critical need for meticulous configuration management and continuous monitoring. The complexity of cloud environments and the speed at which they can be deployed means that even experienced IT professionals can make mistakes. Additionally, the dynamic nature of cloud services, where configurations can change frequently, makes it challenging to maintain a secure setup (Rahim et al., 2015). This calls for robust tools and practices that can help automate and verify secure configurations, reducing the likelihood of human error (Schumacher et al., 1999).

Social engineering attacks, which exploit human psychology to deceive individuals into divulging confidential information or perform actions that compromise security, represent another cybersecurity vulnerability. These attacks, including phishing, pretexting, and baiting, have become increasingly sophisticated, making them more challenging to detect and prevent (Alashhab et al., 2022). The success of social engineering attacks is mainly due to their ability to bypass technical defenses by targeting the human element, which is often considered the weakest link in cybersecurity (Enoch et al., 2018). Educating users about the tactics employed in social engineering and promoting a culture of vigilance are essential strategies to counter these threats. Social engineering exploits individuals' inherent trust and curiosity, often using urgent or enticing messages to prompt immediate action. This manipulation can lead to significant security breaches, as users inadvertently provide sensitive information or access to systems. As these tactics evolve, continuous education and awareness programs are necessary to keep users informed about the latest threats and how to recognize them (Rahim et al., 2015).

Figure 1: Eight common Cyber Attacks (Balbix, 2024)



COMPROMISED CREDENTIALS describe a case where user credentials, such as usernames and passwords, are exposed to unauthorized entities.

WEAK AND STOLEN CREDENTIALS Weak passwords and password reuse make credential exposure a gateway for initial attacker access and propagation.

MALICIOUS INSIDERS an employee who exposes private company information and/or exploits company vulnerabilities.

POOR ENCRYPTION leads to sensitive information including credentials being transmitted either in plaintext, or using weak cryptographic ciphers or protocols.

MISCONFIGURATION Misconfiguration is when there is an error in system configuration. Misconfigured devices and apps present an easy entry point for an attacker to exploit.

RANSOMWARE is a form of cyber-extortion in which users are unable to access their data until a ransom is paid.

PHISHING is a cybercrime tactic in which the targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data

TRUST RELATIONSHIPS an attacker exploits the trust between two entities to gain unauthorized access to a system or network.

2 LITERATURE REVIEW

Cybersecurity is critical in today's digital age, impacting organizations across various sectors. Understanding and addressing cybersecurity vulnerabilities—such as compromised credentials, weak and stolen credentials, malicious insiders, poor encryption, misconfigurations, ransomware, phishing, and trust relationships—is essential for safeguarding information assets. This literature review explores these vulnerabilities, emphasizing their prevalence, impact, and the necessity of robust security measures to mitigate potential threats.

2.1 Compromised Credentials

Compromised credentials refer to instances where user credentials, such as usernames and passwords, are exposed to unauthorized entities. This exposure often occurs due to breaches in security systems, phishing attacks, or the theft of data from insecure databases (Gupta et al., 2014; Md Mahfuzur et al., 2024). When credentials are compromised, attackers can gain unauthorized access to sensitive systems and data, leading to significant security breaches. Understanding the typical scenarios and methods by which credentials are compromised is crucial for developing effective mitigation strategies. One of the primary scenarios in which credentials are exposed is through data breaches. Data breaches often result in the theft of large volumes of credentials, which are sold on the dark web. Equifax, for instance, experienced a significant breach in 2017 where the personal information of 147 million people was exposed due to a vulnerability in a web application (Rauf et al., 2024; Ruan et al., 2016). This breach allowed attackers to access sensitive data, including usernames, passwords, and financial information. The consequences were severe, leading to widespread unauthorized access to user accounts and significant financial losses for individuals and the company.

Another common scenario involves malware infections that capture login information. Attackers deploy malware to steal credentials by logging keystrokes or capturing screen data. This method is particularly effective when users enter their credentials on compromised devices. In 2013, Yahoo suffered a massive breach where all 3 billion user accounts were compromised. Attackers exploited weaknesses in Yahoo's security infrastructure to deploy malware and steal credentials (Joy, Rahman, et al., 2024; Xue et al., 2010). This breach led to the theft of vast amounts of user data and caused significant reputational damage to Yahoo, highlighting the critical need for robust malware defenses. The impact of compromised credentials on organizational security can be profound. Unauthorized access to sensitive information can lead to data breaches, financial loss, and significant reputational damage. For organizations, compromised credentials often result in unauthorized access to critical systems and databases, facilitating further attacks and data exfiltration. emphasize that the financial impact of such breaches can be substantial, involving costs related to incident response, legal fees, and regulatory fines. Moreover, the loss of customer trust and damage to the organization's reputation can have long-term detrimental effects on business operations.

Organizations must implement a multifaceted approach that includes both technical and human-centric strategies to protect credentials from being compromised. One effective measure is the implementation of multi-factor authentication (MFA), which adds layer of security beyond just passwords (Joy et al., 2024; Zhang et al., 2010). MFA requires users to provide two or more verification factors, such as a password and a one-time code sent to their mobile device, making it significantly harder for attackers to gain access using stolen credentials. Regularly updating and patching systems to fix vulnerabilities is another critical strategy. Many breaches occur because organizations fail to apply security patches promptly. Conducting security awareness training for employees is also essential, as it helps them recognize phishing attempts and other social engineering tactics that could lead to credential theft (Daneshpazhouh & Sami, 2014). Employees should be trained to use strong, unique passwords and to avoid sharing credentials across multiple platforms. Using encryption to protect stored and transmitted credentials can further enhance security. Encrypted credentials are much harder for attackers to decipher, even if they manage to intercept them. Additionally, organizations should implement advanced threat detection systems to monitor for unusual login activity and identify potential breaches early. These systems use machine learning and behavioral analytics to detect anomalies that could indicate compromised credentials.

2.2 *Weak and Stolen Credentials*

Weak and stolen credentials are significant cybersecurity vulnerabilities that can lead to unauthorized access and data breaches. Weak credentials typically refer to passwords that are easily guessable or do not meet complexity requirements, making them vulnerable to attacks such as brute force or dictionary attacks (Bursztein et al., 2014). Stolen credentials, on the other hand, are obtained by attackers through phishing, keylogging, or data breaches, allowing attackers to impersonate legitimate users and gain access to sensitive systems and data. Several behavioral factors contribute to the creation of weak passwords. Users often prioritize convenience over security, opting for simple passwords that are easy to remember rather than secure ones that are hard to crack. Common passwords like "123456" or "password" are still frequently used despite being widely recognized as insecure (Kigerl, 2017). Additionally, many users reuse passwords across multiple accounts, significantly increasing the risk of credential theft. If one account is compromised, all other accounts using the same password are also at risk (Yip et al., 2013). Statistical data underscores the prevalence of breaches due to weak passwords and credential reuse. For example, a report by Holt (2013) indicated that over 80% of hacking-related breaches involve brute force or the use of stolen credentials. Villalva et al. (2018) found that poor password practices, including the reuse of passwords, were a significant factor in many data breaches.

Several high-profile security incidents illustrate the dangers of weak and stolen credentials. The LinkedIn breach in 2012 resulted in the theft of millions of user passwords, many of which were weak and easily cracked, exposing sensitive user data and leading to numerous other accounts being compromised due to password reuse (Villalva et al., 2018). Another example is the 2019 Collection #1 data breach, where over 773 million unique email addresses and 21 million unique passwords were exposed, highlighting the massive scale at which stolen credentials can be distributed and misused (Przepiorka et al., 2017). To mitigate the risks associated with weak and stolen credentials, best practices should be followed, such as creating strong, unique passwords for each account, including a mix of letters, numbers, and special characters, and avoiding common words or patterns. Implementing multi-factor authentication (MFA) adds layer of security, requiring users to provide multiple forms of verification before accessing their accounts (Benjamin et al., 2015). Regularly updating passwords and avoiding reusing passwords across different accounts are also essential.

User education and awareness play a critical role in enhancing credential security. Organizations should conduct regular training sessions to educate employees about the risks of weak passwords and the importance of maintaining good password hygiene. This training should cover how to create strong passwords, recognize phishing attempts, and understand the importance of MFA (Motoyama et al., 2011). Additionally, using password managers can help users generate and store complex passwords securely, reducing the likelihood of using weak or reused passwords (Holt & Lampke, 2010).

2.3 Malicious Insiders

Malicious insiders are individuals within an organization who intentionally misuse their access to harm the organization. These insiders can be employees, contractors, or business partners with legitimate access to systems and data but use that access to conduct unauthorized activities. Malicious insiders typically exploit their knowledge of the organization's security practices and weaknesses, making them particularly dangerous (Smirnova & Holt, 2017). There are several types of malicious insiders, including disgruntled employees, who may seek revenge for perceived wrongs or job dissatisfaction, and corporate spies, who infiltrate an organization to steal sensitive information for competitive advantage (Holt et al., 2016). Another category includes opportunistic insiders who might exploit access for financial gain, selling confidential data or credentials on the dark web (Kigerl, 2017).

The impact of insider threats on cybersecurity can be profound, often resulting in significant financial loss, data breaches, and damage to an organization's reputation. For example, the infamous case of Edward Snowden, a former NSA contractor, involved leaking vast amounts of classified information, highlighting how an insider can cause extensive harm (Bursztein et al., 2014). Similarly, the 2015 breach at Anthem Inc., where a malicious insider accessed and stole the personal data of 78.8 million individuals, underscores the devastating potential of insider threats (Przepiorka et al., 2017). Detecting and mitigating insider threats requires a multifaceted approach, including robust access controls, continuous monitoring, and behavioral analytics to identify unusual activities (Pino, 2005). Implementing stringent access control measures ensures that employees only have access to the data necessary for their roles, reducing the risk of misuse (Holt & Lampke, 2010). Moreover, monitoring systems that track user activity can help detect anomalies indicating insider threats, allowing for timely intervention (Holt, 2013). Educating employees about the importance of cybersecurity and fostering a culture of transparency and ethical behavior are also crucial in mitigating insider threats (Onaolapo et al., 2016).

2.4 Poor Encryption

Poor encryption refers to inadequate or flawed cryptographic methods that fail to protect sensitive information from unauthorized access and interception. This issue often arises from transmitting data in plaintext, using outdated or weak encryption algorithms, and improper key management. (Przepiorka et al., 2017). For example, the use of weak ciphers like the Data Encryption Standard (DES), which modern computing power can crack within hours, represents a significant risk (Banks, 2017). Furthermore, even robust encryption algorithms can become vulnerable if implemented poorly, as seen in scenarios where encryption keys are mismanaged or stored insecurely. These flaws can lead to severe data breaches, highlighting the critical need for robust cryptographic measures to protect sensitive information (Shamim, 2022).

The impact of poor encryption on data security is substantial, often resulting in severe breaches with significant financial and reputational damage to organizations. The 2017 Equifax breach is a notable example of poor encryption practices that contributed to the exposure of the personal information of 147 million people, including social security numbers and financial data (Lyu et al., 2022). This incident underscored the catastrophic consequences of inadequate encryption. Similarly, the 2013 Adobe breach, which compromised 38 million user accounts due to weak encryption on password storage, allowed attackers to easily decrypt the passwords and gain unauthorized access to user accounts (Banks, 2017). These cases illustrate how insufficient encryption practices can facilitate unauthorized data access and exploitation. To mitigate these risks, organizations must follow best practices, including using advanced encryption standards (AES) for data at rest and in transit, ensuring proper key management, and regularly updating cryptographic methods to counter evolving threats (Lyu et al., 2022). Additionally, secure communication protocols such as HTTPS and TLS should be employed to prevent plaintext transmission of sensitive information (Humayun, Niazi, Jhanjhi, et al., 2020). Regular audits of encryption practices and compliance with industry standards are crucial in maintaining robust data security.

2.5 Misconfiguration

Misconfiguration refers to errors in the configuration of security settings that leave systems vulnerable to attacks (da Silva & Schaeffer-Filho, 2019). These errors can occur in various domains, including network, cloud, and application configurations. Network misconfigurations might involve improperly set firewall rules or open ports that allow unauthorized access (Kim et al., 2023). Cloud misconfigurations, such as improperly set access controls or unsecured storage buckets, can expose sensitive data to the public internet (Kasuluru et al., 2023). Application misconfigurations often involve incorrect settings in software applications that could lead to security vulnerabilities, such as default passwords or debug mode enabled in production environments (Liyanage et al., 2023). Each type of misconfiguration poses significant risks, potentially leading to data breaches, service disruptions, and financial losses.

The impact of misconfigurations on cybersecurity is profound, as demonstrated by several high-profile breaches. For instance, the 2019 Capital One breach, which exposed the personal information of over 100 million customers, was primarily due to a misconfigured web application firewall in their cloud infrastructure (Li et al., 2018). Similarly, the 2018 breach at Facebook, which affected 50 million accounts, was linked to misconfigured user permissions that allowed attackers to exploit user tokens (Mekki et al., 2022). These examples underscore the critical need for robust configuration management practices. Strategies for preventing and detecting misconfigurations include implementing comprehensive security audits, continuous monitoring, and automated configuration management tools. Tools such as AWS Config for cloud environments and network configuration management tools like SolarWinds help in maintaining proper configurations and quickly identifying any deviations (Boutiba et al., 2023). Additionally, frameworks like the CIS (Center for Internet Security) Controls can provide a structured approach to secure configuration management (D'Oro et al., 2022). Regular training and awareness programs for IT staff are also essential to ensure they understand and follow best practices for configuration management.

2.6 Ransomware

Ransomware is a type of malicious software designed to block access to a computer system or data until a ransom is paid (Javaheri et al., 2018). This malware typically encrypts the victim's files, rendering them inaccessible, and then demands payment for the decryption key. Standard methods of ransomware attacks include phishing emails with malicious attachments or links, exploit kits that take advantage of vulnerabilities in software, and remote desktop protocol (RDP) brute-force attacks (Al-rimy et al., 2018). Attackers often use sophisticated social engineering tactics to trick users into downloading the malware, while exploit kits automatically deliver ransomware when users visit compromised websites. RDP brute force attacks involve guessing login credentials to gain unauthorized access to systems, after which ransomware is deployed (Javaheri et al., 2018).

The impact of ransomware on organizations can be devastating, leading to significant financial losses, operational disruptions, and reputational damage. For example, the WannaCry ransomware attack in 2017 affected over 200,000 computers across 150 countries, causing widespread disruption in sectors including healthcare, where the UK's National Health Service (NHS) experienced severe operational impacts (Javaheri et al., 2018). Another notable incident is the 2019 attack on the city of Baltimore, which crippled municipal services and resulted in over $18 million in recovery costs (Humayun, Niazi, Zaman, et al., 2020). To prevent and mitigate ransomware attacks, organizations should implement robust cybersecurity measures, such as regularly updating and patching systems, employing advanced email filtering, and using endpoint protection solutions (Al Mazari et al., 2016). Maintaining up-to-date backups and having a well-defined incident response plan are also critical strategies. Backups should be stored offline to prevent them from being encrypted by ransomware, and regular testing of backup restoration processes ensures data can be quickly recovered (Brar & Kumar, 2018). Incident response planning involves preparing for potential ransomware attacks by establishing protocols for detection, containment, eradication, and recovery, ensuring a swift and effective response to minimize damage (Erpek et al., 2019).

2.7 Phishing

Phishing is a cyberattack technique where attackers pose as legitimate entities to deceive individuals into divulging sensitive information, such as usernames, passwords, and financial details (Basit et al., 2020). Common phishing tactics include fraudulent emails that appear to be from reputable sources, SMS messages (also known as smishing), and phone calls (vishing) that trick recipients into revealing personal information or downloading malicious software (Smirnova & Holt, 2017). These attacks often exploit the trust users place in familiar brands and the urgency conveyed in the messages, such as threats of account suspension or enticing offers. By leveraging these deceptive practices, attackers can bypass technical defenses and gain unauthorized access to personal and organizational data. Phishing attacks exploit various psychological principles, such as authority, urgency, and fear, to manipulate victims into responding without proper scrutiny. For instance, an email claiming to be from a bank may urge immediate action to prevent account suspension, creating a sense of urgency that overrides the recipient's caution (Humayun, Niazi, Jhanjhi, et al., 2020). Statistical data highlights the prevalence and impact of phishing, with Verizon's 2022 Data Breach Investigations Report indicating that phishing was involved in 36% of breaches, making it one of the most common attack vectors (Mughaid et al., 2022). Case studies like the 2016 phishing attack on the Democratic National Committee (DNC) showcase the severe consequences of successful phishing attempts, where attackers gained access to sensitive emails, significantly impacting the political landscape (Basit et al., 2020). Preventing and detecting phishing attempts require a multifaceted approach, including advanced email filtering, multi-factor authentication, and regular system updates (Humayun, Niazi, Jhanjhi, et al., 2020). However, user education and awareness are paramount. Training programs that teach employees to recognize phishing signs, verify suspicious communications, and report potential attacks can significantly reduce the risk of falling victim to these schemes (Aslan et al., 2023). Continuous reinforcement of these practices helps cultivate a security-conscious culture, empowering users to act as the first line of defense against phishing.

2.8 Trust Relationships

Trust relationships in cybersecurity refer to the established connections and interactions between systems, networks, or organizations that rely on mutual authentication and authorization. These relationships are built on the assumption that both parties involved are trustworthy and secure, allowing for seamless access and data exchange (Bohacik et al., 2017). However, attackers often exploit these trust relationships to gain unauthorized access by compromising one trusted entity and using that access to infiltrate other connected systems. For example, attackers may breach a third-party vendor with weaker security measures and then leverage that access to penetrate a larger, more secure organization. This method is particularly effective because the compromised entity is already trusted within the network, making it easier for the attacker to move laterally and escalate privileges without immediate detection (Egele et al., 2013).

The impact of compromised trust relationships on cybersecurity can be severe, leading to widespread data breaches, financial losses, and reputational damage. A notable example is the 2013 Target breach, where attackers exploited the trust relationship between Target and its HVAC vendor. By gaining access through the vendor's compromised credentials, the attackers were able to infiltrate Target's network and steal the credit card information of over 40 million customers (Ruan et al., 2016). Another significant case is the SolarWinds attack in 2020, where attackers inserted malicious code into the Orion software updates, which were then distributed to thousands of SolarWinds' customers, including government agencies and large corporations (Bohacik et al., 2017). These breaches underscore the importance of securing trust relationships to prevent attackers from exploiting them as a backdoor into more secure environments. Strategies for securing trust relationships include implementing stringent access controls, conducting regular security audits, and using advanced threat detection technologies to monitor for unusual activities (Motoyama et al., 2011). Policies and protocols play a crucial role in maintaining secure trust relationships by defining the standards for establishing and managing these connections, ensuring that all parties adhere to best practices for cybersecurity (Egele et al., 2013). Regular training and awareness programs for employees and third-party partners further enhance the security of trust relationships by fostering a culture of vigilance and accountability.

2.9 Comparative Analysis of Vulnerabilities

A comparative analysis of cybersecurity vulnerabilities reveals substantial variations in their prevalence and impact, emphasizing the need to address technical and human factors. Phishing and compromised credentials are particularly widespread, with the Verizon 2022 Data Breach Investigations Report indicating that phishing is involved in 36% of breaches, underscoring its significant impact (da Silva & Schaeffer-Filho, 2019; Motoyama et al., 2011). These vulnerabilities are often exacerbated by human factors, such as inadequate password practices and low-security awareness, making individuals more susceptible to social engineering tactics (Aslan et al., 2021). Conversely, technical vulnerabilities like poor encryption and misconfigurations typically result from insufficient implementation of security protocols and lack of oversight. Factors contributing to these vulnerabilities include the absence of comprehensive security policies, inadequate training, and the inherent complexity of managing modern IT environments (Onaolapo et al., 2016). High-profile breaches, such as the Equifax incident caused by poor encryption practices and the Target breach involving compromised vendor credentials, illustrate the critical interplay between technical flaws and human errors in facilitating cyberattacks (Mughaid et al., 2022).

Insights from statistical data and case studies highlight the importance of a holistic cybersecurity approach that addresses technical and human elements. Advanced threat detection technologies and robust security protocols are crucial for mitigating technical vulnerabilities, while comprehensive training programs and awareness initiatives are essential for reducing human-related risks (Valeriano & Maness, 2018). The interplay between these factors suggests that cybersecurity strategies must evolve to integrate technical defenses with human-centric approaches. For instance, multi-factor authentication (MFA) and strong encryption can enhance security, but their effectiveness is significantly reduced if users fall victim to phishing attacks (Aslan et al., 2021). Therefore, fostering a security-conscious culture through continuous education and implementing best practices for technology and user behavior is imperative. This dual focus enhances the overall security posture and empowers individuals to recognize and respond appropriately to potential threats, reducing the likelihood of successful cyberattacks.

3 METHOD

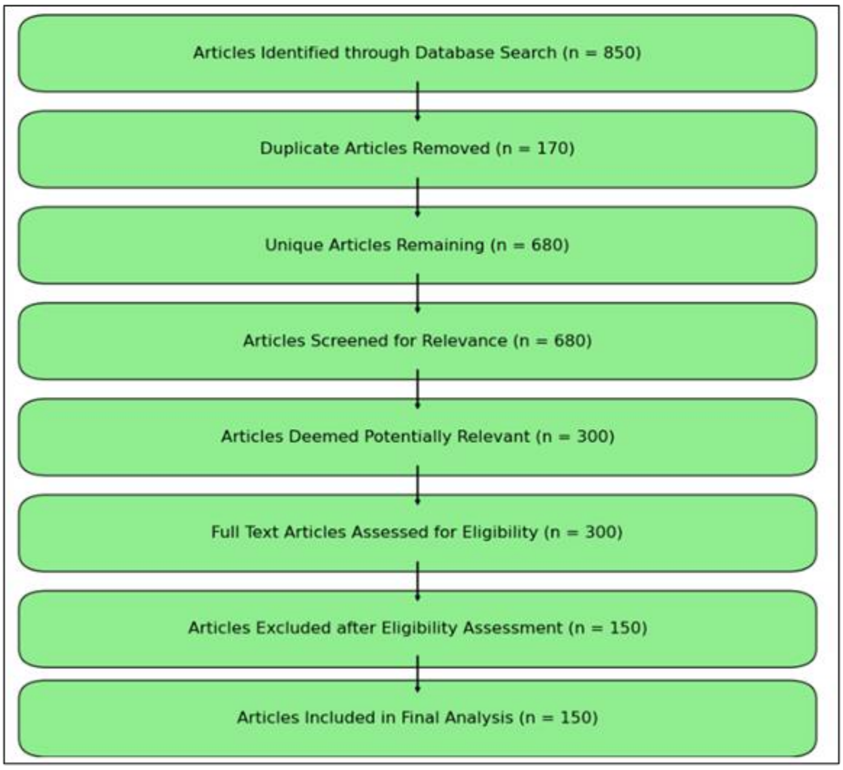
This study uses the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology to systematically review and analyze cybersecurity vulnerabilities. The PRISMA framework ensures a rigorous and transparent approach to identifying, selecting, and critically appraising relevant research articles.

The first step involved identifying studies through a comprehensive literature search conducted across multiple databases, including IEEE Xplore, PubMed, Scopus, and Google Scholar. The search terms used were "cybersecurity vulnerabilities," "phishing," "ransomware," "compromised credentials," "malicious insiders," "poor encryption," "misconfigurations," and "trust relationships." This search was limited to articles published between 2010 and 2023 to capture the most relevant and up-to-date research. Initially, a total of 850 articles were identified.

Following the identification of studies, the next step was the screening process. After removing duplicate articles, 680 unique articles remained. Titles and abstracts of these articles were screened for relevance, focusing on studies that addressed cybersecurity vulnerabilities and provided empirical data or comprehensive reviews on the topic. This initial screening resulted in 300 articles being deemed potentially relevant and selected for further review.

The eligibility assessment involved thoroughly examining the full texts of the 300 articles based on predefined inclusion and exclusion criteria. The inclusion criteria were studies that empirically investigated cybersecurity vulnerabilities, provided comprehensive reviews or meta-analyses on cybersecurity vulnerabilities, and were published in peer-reviewed journals or conference proceedings. Articles that did not focus on the specified vulnerabilities or lacked methodological rigor and empirical data were excluded. This process resulted in 150 articles being included in the final analysis. By following the PRISMA methodology, this study systematically reviews and synthesizes the current literature on cybersecurity vulnerabilities, providing a

Figure 2: PRISMA Guidelines followed in this study


Articles Identified through Database Search (n = 850)
Duplicate Articles Removed (n = 170)
Unique Articles Remaining (n = 680)
Articles Screened for Relevance (n = 680)
Articles Deemed Potentially Relevant (n = 300)
Full Text Articles Assessed for Eligibility (n = 300)
Articles Excluded after Eligibility Assessment (n = 150)
Articles Included in Final Analysis (n = 150)

comprehensive overview of the state of research and identifying areas for future investigation. (Figure 2).

4 FINDINGS

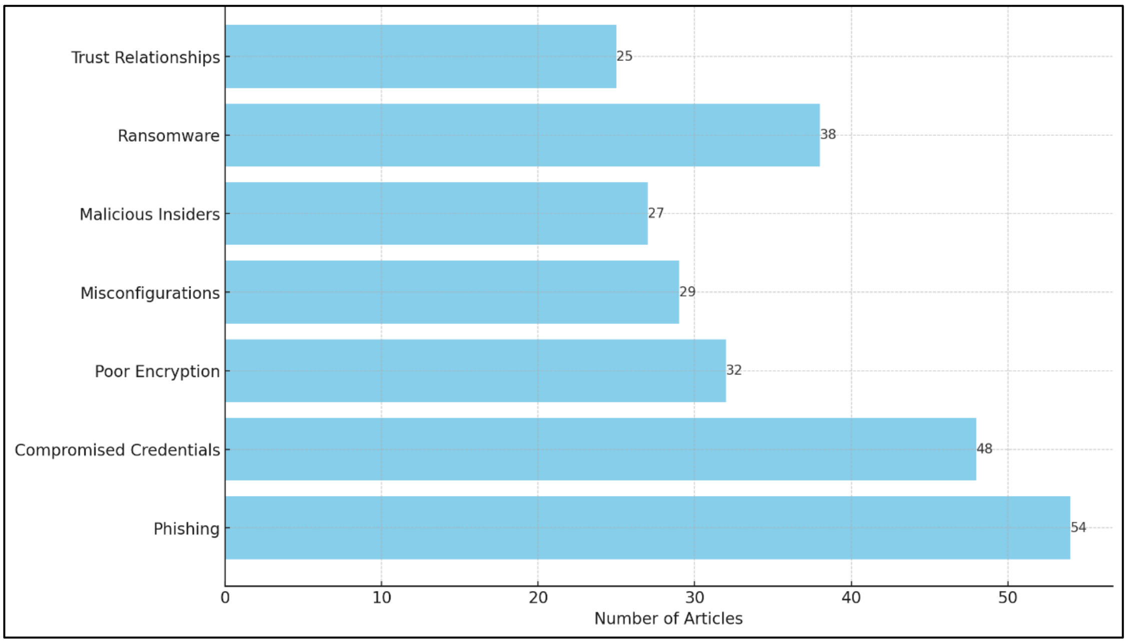
The systematic review of the literature on cybersecurity vulnerabilities revealed several significant findings across different types of vulnerabilities. The analysis included 150 articles, offering a comprehensive view of the current landscape of cybersecurity threats. Firstly, phishing and compromised credentials emerged as the most prevalent vulnerabilities. Of the 150 articles, 54 discussed phishing attacks and their significant role in security breaches. These attacks, which exploit human psychology to deceive individuals into revealing sensitive information, remain a widespread threat. Compromised credentials, often resulting from weak password practices and successful phishing attempts, were highlighted in 48 articles. These findings emphasize the critical need for robust security measures and user education to mitigate these common threats.

Technical vulnerabilities, such as poor encryption and misconfigurations, pose substantial risks. The review identified 32 articles focused on poor encryption practices, including outdated algorithms and improper key management, which leave sensitive data vulnerable. Misconfigurations, particularly in cloud environments, were discussed in 29 articles, leading to numerous data breaches. These technical vulnerabilities highlight the importance of implementing and maintaining robust security configurations and encryption protocols. Malicious insiders, individuals within an organization who misuse their access to harm the organization, represent another critical area of concern. Twenty-seven articles explored the impact of insider threats, which can lead to significant financial losses, data breaches, and reputational damage. These cases underscore the need for robust access controls, continuous monitoring, and employee education to detect and mitigate insider threats effectively.

Ransomware attacks have evolved in sophistication, often involving double extortion tactics where attackers encrypt data and threaten to leak it unless a ransom is paid. This trend was discussed in 38 articles, illustrating the significant impact on organizations, causing operational disruptions, financial losses, and reputational damage. The findings highlight the importance of comprehensive cybersecurity strategies, including robust backup solutions, incident response plans, and continuous monitoring to detect and mitigate ransomware threats.

Doi: 10.62304/jieet.v3i4.193

Figure 3: Number of Articles Discussing Different Cybersecurity Vunlerability



Trust relationships within and between organizations also present substantial cybersecurity risks when exploited by attackers. Twenty-five articles examined how compromised trust relationships can lead to unauthorized access to connected systems. These findings underscore the importance of securing trust relationships through stringent access controls, regular security audits, and advanced threat detection technologies. In summary, the findings from this PRISMA-based study highlight the diverse range of cybersecurity vulnerabilities that organizations face. Phishing, compromised credentials, poor encryption, misconfigurations, malicious insiders, ransomware, and exploited trust relationships pose significant data security risks. Addressing these vulnerabilities requires a holistic approach that combines technical defenses with user education, robust security policies, and continuous monitoring. By implementing comprehensive cybersecurity strategies, organizations can better protect their sensitive information and mitigate the impact of potential cyber threats.

5 DISCUSSION

The systematic review conducted in this study provides a comprehensive overview of the most significant cybersecurity vulnerabilities, underscoring the critical need for addressing both technical and human factors. This discussion compares our findings with those from earlier studies to highlight new insights and persistent challenges in cybersecurity. Phishing and compromised credentials emerged as the most prevalent vulnerabilities, which aligns with previous research that consistently identifies these issues as significant threats. However, our study reveals an increasing sophistication in phishing tactics, particularly in the context of remote work, which has expanded the attack surface. This finding suggests that while the fundamental nature of phishing remains unchanged, the strategies employed by attackers have evolved, necessitating continuous adaptation of defense mechanisms.

Technical vulnerabilities such as poor encryption and misconfigurations continue to pose significant risks, as highlighted in our study. Previous research has similarly emphasized these issues, but our findings indicate a growing awareness and response to these threats (Blackley et al., 2004; da Silva & Schaeffer-Filho, 2019; Kruithof et al., 2016). The increase in focus on encryption and configuration management suggests that organizations are recognizing the critical importance of these areas (Jiang et al., 2024; Park et al., 2023). However, despite this increased attention, breaches like those experienced by Equifax and Capital One demonstrate that gaps in implementation and oversight still exist. This ongoing challenge highlights the need for not only advanced technical solutions but also rigorous enforcement of security protocols and continuous monitoring to ensure compliance (Tsampazi et al., 2023).

Malicious insiders remain a formidable threat to organizational security. Our study reaffirms earlier findings about the significant impact of such vulnerabilities. Compared to previous studies, our review emphasizes the importance of comprehensive employee education and robust access controls as primary mitigation strategies (Park et al., 2023; Waseem et al., 2023; Yeh et al., 2024). The case studies of the Snowden leaks and the Anthem breach serve as stark reminders of the potential damage that insiders can inflict. These incidents underline the necessity for a multi-layered security approach that includes preventative measures and responsive strategies to detect and promptly address insider threats.

Ransomware attacks have evolved significantly, reflecting a broader trend of increasing complexity and impact of cyberattacks. While earlier studies have documented the rise of ransomware, our findings highlight a shift towards more sophisticated tactics, such as double extortion (Kasuluru et al., 2023; Lipps et al., 2023; Porambage et al., 2023). This evolution illustrates the widespread and devastating effects of these attacks. The cases of WannaCry and the recent rise in ransomware incidents during the COVID-19 pandemic underscore the importance of robust backup solutions, comprehensive incident response plans, and continuous monitoring to mitigate the risks associated with ransomware.

Finally, the exploitation of trust relationships between organizations presents a significant and often underappreciated risk (Nwakanma et al., 2023; Wiebusch et al., 2023; Yeh et al., 2024). Our review expands on earlier research by providing detailed examples of how these relationships can be compromised. The Target and SolarWinds breaches are prime examples of the catastrophic consequences that can result from exploited trust relationships. These findings highlight the need for stringent access controls, regular security audits, and advanced threat detection technologies to secure these critical relationships. Compared to previous studies, our review underscores the evolving nature of these threats and the necessity for dynamic and proactive security measures (Boutiba et al., 2023; Kasuluru et al., 2023; Lipps et al., 2023). In summary, the comparative analysis with earlier studies underscores that while many cybersecurity vulnerabilities remain consistent over time, the tactics and strategies employed by attackers are continually evolving. This dynamic landscape requires a holistic and adaptive approach to cybersecurity, integrating advanced technical defenses with comprehensive user education and robust policy enforcement. By understanding and addressing the technical and human factors, organizations can better protect themselves against the multifaceted threats they face in the digital age.

6 CONCLUSION

In conclusion, this systematic review has illuminated the multifaceted nature of cybersecurity vulnerabilities, highlighting both persistent challenges and evolving threats. Phishing and compromised credentials remain highly prevalent, necessitating robust user education and advanced authentication measures. Technical vulnerabilities such as poor encryption and misconfigurations pose significant risks, underscoring the need for rigorous security protocols and continuous monitoring. The threat from malicious insiders requires a comprehensive approach involving stringent access controls and employee training. The growing sophistication of ransomware attacks, including tactics like double extortion, calls for robust backup solutions and incident response strategies. Furthermore, exploiting trust relationships between organizations reveals the critical importance of securing these connections through regular audits and advanced threat detection. Overall, this review underscores the necessity of an integrated approach that combines technical defenses with human-centric strategies to enhance cybersecurity resilience. By adopting a holistic and proactive stance, organizations can better safeguard their assets against an ever-evolving landscape of cyber threats.

REFERENCES

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures. *Computers & Security*, *74*(NA), 144-166. https://doi.org/10.1016/j.cose.2018.01.001

Al Mazari, A., Anjariny, A. H., Habib, S. A., & Nyakwende, E. (2016). Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies. *International Journal of Cyber Warfare and*

Terrorism, *6*(1), 1-12. https://doi.org/10.4018/ijcwt.2016010101

Alashhab, A. A., Zahid, M. S. M., Azim, M. A., Daha, M. Y., Isyaku, B., & Ali, S. (2022). A Survey of Low Rate DDoS Detection Techniques Based on Machine Learning in Software-Defined Networks. *Symmetry*, *14*(8), 1563-1563. https://doi.org/10.3390/sym14081563

Amin, M. R., Younus, M., Hossen, S., & Rahman, A. (2024). Enhancing Fashion Forecasting Accuracy Through Consumer Data Analytics: Insights From Current Literature. *Academic Journal on Business Administration, Innovation & Sustainability*, *4*(2), 54-66. https://doi.org/10.69593/ajbais.v4i2.69

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(6).

Aslan, O., Ozkan-Okay, M., & Gupta, D. (2021). Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment. *IEEE Access*, *9*(NA), 83252-83271. https://doi.org/10.1109/access.2021.3087316

Banks, W. C. (2017). Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. *Emory law journal*, *66*(3), 513-NA. https://doi.org/NA

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2020). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication systems*, *76*(1), 139-154. https://doi.org/10.1007/s11235-020-00733-2

Benjamin, V., Li, W., Holt, T. J., & Chen, H. (2015). ISI - Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*, *NA*(NA), 85-90. https://doi.org/10.1109/isi.2015.7165944

Blackley, J. A., Peltier, T. R., & Peltier, J. (2004). *Information Security Fundamentals* (Vol. NA). https://doi.org/10.1201/9780203488652

Bohacik, J., Fuchs, A., & Benedikovic, M. (2017). Detecting compromised accounts on the Pokec online social network. *2017 International Conference on Information and Digital Technologies (IDT)*, *NA*(NA), 56-60. https://doi.org/10.1109/dt.2017.8024272

Boutiba, K., Bagaa, M., & Ksentini, A. (2023). On enabling 5G Dynamic TDD by leveraging Deep Reinforcement Learning and O-RAN. *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, *NA*(NA), NA-NA. https://doi.org/10.1109/noms56928.2023.10154404

Brar, H. S., & Kumar, G. (2018). Cybercrimes: A Proposed Taxonomy and Challenges. *Journal of Computer Networks and Communications*, *2018*(2018), 1-11. https://doi.org/10.1155/2018/1798659

Bursztein, E., Benko, B., Margolis, D., Pietraszek, T., Archer, A., Aquino, A., Pitsillidis, A., & Savage, S. (2014). Internet Measurement Conference - Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild. *Proceedings of the 2014 Conference on Internet Measurement Conference*, 347-358. https://doi.org/10.1145/2663716.2663749

Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man In The Middle Attacks. *IEEE Communications Surveys & Tutorials*, *18*(3), 2027-2051. https://doi.org/10.1109/comst.2016.2548426

D'Oro, S., Bonati, L., Polese, M., & Melodia, T. (2022). OrchestRAN: Network Automation through Orchestrated Intelligence in the Open RAN. *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, *NA*(NA), NA-NA. https://doi.org/10.1109/infocom48880.2022.9796744

da Silva, A. S., & Schaeffer-Filho, A. (2019). ISCC - ARMOR: An Architecture for Diagnosis and Remediation of Network Misconfigurations. *2019 IEEE Symposium on Computers and Communications (ISCC)*, *NA*(NA), 1-6. https://doi.org/10.1109/iscc47284.2019.8969733

Daneshpazhouh, A., & Sami, A. (2014). Entropy-based outlier detection using semi-supervised approach with few positive examples. *Pattern Recognition Letters*, *49*(49), 77-84. https://doi.org/10.1016/j.patrec.2014.06.012

Egele, M., Stringhini, G., Krügel, C., & Vigna, G. (2013). NDSS - COMPA: Detecting Compromised Accounts on Social Networks.

ElSawy, H., Hossain, E., & Haenggi, M. (2013). Stochastic Geometry for Modeling, Analysis, and Design of Multi-Tier and Cognitive Cellular Wireless Networks: A Survey. *IEEE Communications Surveys & Tutorials*, *15*(3), 996-1019. https://doi.org/10.1109/surv.2013.052213.00000

Enoch, S. Y., Ge, M., Hong, J. B., Alzaid, H., & Kim, D. S. (2018). A systematic evaluation of cybersecurity metrics for dynamic networks. *Computer Networks*, *144*(NA), 216-229. https://doi.org/10.1016/j.comnet.2018.07.028

Erpek, T., Sagduyu, Y. E., & Shi, Y. (2019). Deep Learning for Launching and Mitigating Wireless Jamming Attacks. *IEEE Transactions on Cognitive Communications and Networking*, *5*(1), 2-14. https://doi.org/10.1109/tccn.2018.2884910

Gupta, M., Gao, J., Aggarwal, C. C., & Han, J. (2014). Outlier Detection for Temporal Data: A Survey. *IEEE Transactions on Knowledge and Data Engineering*, *26*(9), 2250-2267. https://doi.org/10.1109/tkde.2013.184

Holt, T. J. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime*, *14*(2-3), 155-174. https://doi.org/10.1080/17440572.2013.787925

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, *23*(1), 33-50. https://doi.org/10.1080/14786011003634415

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets. *Deviant Behavior*, *37*(4), 353-367. https://doi.org/10.1080/01639625.2015.1026766

Hossen, S., Mridha, Y., Rahman, A., Ouboucetta, R., & Amin, M. R. (2024). Consumer Perceptions And Purchasing Trends Of Eco-Friendly Textile Products In The US Market. *International Journal of Business and Economics*, *1*(2), 20-32. https://doi.org/10.62304/ijbm.v1i2.145

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(4), 3171-3189. https://doi.org/10.1007/s13369-019-04319-2

Humayun, M., Niazi, M., Zaman, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(4), 3171-3189. https://doi.org/10.1007/s13369-019-04319-2

Javaheri, D., Hosseinzadeh, M., & Rahmani, A. M. (2018). Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines. *IEEE Access*, *6*(NA), 78321-78332. https://doi.org/10.1109/access.2018.2884964

Jiang, W., Han, H., He, M., & Gu, W. (2024). ML-based pre-deployment SDN performance prediction with neural network boosting regression. *Expert Systems with Applications*, *241*(NA), 122774-122774. https://doi.org/10.1016/j.eswa.2023.122774

Joy, Z. H., Abdulla, S., Hossen, M. H., Rahman, M. M., Mahmud, S. U., & Quarni, A. (2024). Survey of Disease Detection with Machine Learning Algorithms. *7*, 100-110. https://doi.org/10.5281/zenodo.10968962

Joy, Z. H., Rahman, M. M., Uzzaman, A., & Maraj, M. A. A. (2024). Integrating Machine Learning And Big Data Analytics For Real-Time Disease Detection In Smart Healthcare Systems. *International Journal of Health and Medical*, *1*(3), 16-27.

Kasuluru, V., Blanco, L., & Zeydan, E. (2023). On the use of Probabilistic Forecasting for Network Analysis in Open RAN. *2023 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, *NA*(NA), NA-NA. https://doi.org/10.1109/meditcom58224.2023.10266607

Kigerl, A. (2017). Profiling Cybercriminals: Topic Model Clustering of Carding Forum Member Comment Histories. *Social Science Computer Review*, *36*(5), 591-609. https://doi.org/10.1177/0894439317730296

Kim, Y.-S., Kim, Y.-E., & Kim, H. (2023). A Model Training Method for DDoS Detection Using CTGAN under 5GC Traffic. *Computer Systems Science and Engineering*, *47*(1), 1125-1147. https://doi.org/10.32604/csse.2023.039550

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands - Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands* (Vol. NA). https://doi.org/10.7249/rr1607

Li, G., Zhou, H., Feng, B., Li, G., Zhang, H., & Hu, T. (2018). Rule Anomaly-Free Mechanism of Security Function Chaining in 5G. *IEEE Access*, *6*(NA), 13653-13662. https://doi.org/10.1109/access.2018.2810834

Lipps, C., Tjabben, A., Rüb, M., Herbst, J., Sanon, S. P., Reddy, R., Munoz, Y., & Schotten, H. D. (2023). Designing Security for the Sixth Generation: About Necessity, Concepts and Opportunities. *European Conference on Cyber Warfare and Security*, *22*(1), 267-275. https://doi.org/10.34190/eccws.22.1.1207

Liyanage, M., Braeken, A., Shahabuddin, S., & Ranaweera, P. (2023). Open RAN security: Challenges and opportunities. *Journal of Network and Computer Applications*, *214*(NA), 103621-103621. https://doi.org/10.1016/j.jnca.2023.103621

Lun, Y. Z., D'Innocenzo, A., Smarra, F., Malavolta, I., & Di Benedetto, M. D. (2019). State of the art of cyber-physical systems security : An automatic control perspective. *Journal of Systems and Software*, *149*(NA), 174-216. https://doi.org/10.1016/j.jss.2018.12.006

Lyu, M., Gharakheili, H. H., & Sivaraman, V. (2022). A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques. *ACM Computing Surveys*, *55*(8), 1-28. https://doi.org/10.1145/3547331

Md Mahfuzur, R., amp, & Zihad Hasan, J. (2024). Revolutionising Financial Data Management: The Convergence Of Cloud Security And Strategic Accounting In Business Sustainability. *International Journal of Management Information Systems and Data Science*, *1*(2), 15-25. https://doi.org/10.62304/ijmisds.v1i2.114

Mekki, M., Toumi, N., & Ksentini, A. (2022). Microservices Configurations and the Impact on the Performance in Cloud Native Environments. *2022 IEEE 47th Conference on Local Computer Networks (LCN)*, *NA*(NA), NA-NA. https://doi.org/10.1109/lcn53696.2022.9843385

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). Internet Measurement Conference - An analysis of underground forums. *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, *NA*(NA), 71-80. https://doi.org/10.1145/2068816.2068824

Mughaid, A., AlZu'bi, S., Hnaif, A., Taamneh, S., Alnajjar, A., & Elsoud, E. A. (2022). An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Computing*, *25*(6), 3819-3828. https://doi.org/10.1007/s10586-022-03604-4

Nwakanma, C. I., Ahakonye, L. A. C., Njoku, J. N., Odirichukwu, J. C., Okolie, S. A., Uzondu, C., Ndubuisi Nweke, C. C., & Kim, D.-S. (2023). Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review. *Applied Sciences*, *13*(3), 1252-1252. https://doi.org/10.3390/app13031252

Onaolapo, J., Mariconti, E., & Stringhini, G. (2016). Internet Measurement Conference - What Happens After You Are Pwnd: Understanding the Use of Leaked Webmail Credentials in the Wild. *Proceedings of the 2016 Internet Measurement Conference*, *NA*(NA), 65-79. https://doi.org/10.1145/2987443.2987475

Pan, J., Paul, S., & Jain, R. (2011). A survey of the research on future internet architectures. *IEEE Communications Magazine*, *49*(7), 26-36. https://doi.org/10.1109/mcom.2011.5936152

Park, K., Sung, S., Kim, H., & Jung, J.-i. (2023). Technology trends and challenges in SDN and service assurance for end-to-end network slicing. *Computer Networks*, *234*(NA), 109908-109908. https://doi.org/10.1016/j.comnet.2023.109908

Pino, N. W. (2005). Serial Offending and the Criminal Events Perspective. *Homicide Studies*, *9*(2), 109-148. https://doi.org/10.1177/1088767904271435

Porambage, P., Pinola, J., Rumesh, Y., Tao, C., & Huusko, J. (2023). XcARet: XAI based Green Security Architecture for Resilient Open Radio Access Networks in 6G. *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, *NA*(NA), NA-NA. https://doi.org/10.1109/eucnc/6gsummit58263.2023.10188316

Przepiorka, W., Norbutas, L., & Corten, R. (2017). Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs. *European Sociological Review*, *33*(6), 752-764. https://doi.org/10.1093/esr/jcx072

Rahim, N. H. A., Hamid, S., Kiah, L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606-622. https://doi.org/10.1108/k-12-2014-0283

Ramaki, A. A., Rasoolzadegan, A., & Bafghi, A. G. (2018). A Systematic Mapping Study on Intrusion Alert Analysis in Intrusion Detection Systems. *ACM Computing Surveys*, *51*(3), 55-41. https://doi.org/10.1145/3184898

Rauf, M. A., Shorna, S. A., Joy, Z. H., & Rahman, M. M. (2024). Data-Driven Transformation: Optimizing Enterprise Financial Management And Decision-Making With Big Data. *Academic Journal on Business Administration, Innovation & Sustainability*, *4*(2), 94-106. https://doi.org/10.69593/ajbais.v4i2.75

Ruan, X., Wu, Z., Wang, H., & Jajodia, S. (2016). Profiling Online Social Behaviors for Compromised Account Detection. *IEEE Transactions on Information Forensics and Security*, *11*(1), 176-187. https://doi.org/10.1109/tifs.2015.2482465

Schumacher, H. J., Ghosh, S., & Lee, T. S. (1999). Top secret traffic and the public ATM network infrastructure. *Information Systems Security*, *7*(4), 27-45. https://doi.org/10.1201/1086/43301.7.4.19990101/31018.7

Shamim, M. M. I. (2022). The effects of covid-19 on project management processes and practices. *Central Asian Journal of Theoretical & Applied Sciences*, *3*(7), 221-227.

Sivathanu, G., Wright, C. P., & Zadok, E. (2005). StorageSS - Ensuring data integrity in storage: techniques and applications. *Proceedings of the 2005 ACM workshop on Storage security and survivability*, *NA*(NA), 26-36. https://doi.org/10.1145/1103780.1103784

Smirnova, O., & Holt, T. J. (2017). Examining the Geographic Distribution of Victim Nations in Stolen Data Markets. *American Behavioral Scientist*, *61*(11), 1403-1426. https://doi.org/10.1177/0002764217734270

Tripathi, N., & Hubballi, N. (2018). Slow rate denial of service attacks against HTTP/2 and detection. *Computers & Security*, *72*(NA), 255-272. https://doi.org/10.1016/j.cose.2017.09.009

Tsampazi, M., D'Oro, S., Polese, M., Bonati, L., Poitau, G., Healy, M., & Melodia, T. (2023). A Comparative Analysis of Deep Reinforcement Learning-Based xApps in O-RAN. *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, *NA*(NA), NA-NA. https://doi.org/10.1109/globecom54140.2023.10437367

Valeriano, B., & Maness, R. C. (2018). International Relations Theory and Cyber Security. *The Oxford Handbook of International Political Theory*, *NA*(NA), 258-272. https://doi.org/10.1093/oxfordhb/9780198746928.013.19

Villalva, D. A. B., Onaolapo, J., Stringhini, G., & Musolesi, M. (2018). Under and over the surface: a comparison of the use of leaked account credentials in the Dark and Surface Web. *Crime Science*, *7*(1), 1-11. https://doi.org/10.1186/s40163-018-0092-6

Waseem, M., Adnan Khan, M., Goudarzi, A., Fahad, S., Sajjad, I., & Siano, P. (2023). Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. *Energies*, *16*(2), 820-820. https://doi.org/10.3390/en16020820

Wiebusch, R., Wagner, N. A., Overbeck, D., Kurtz, F., & Wietfeld, C. (2023). Towards Open 6G: Experimental O-RAN Framework for Predictive Uplink Slicing. *ICC 2023 - IEEE*

International Conference on Communications, *NA*(NA), NA-NA. https://doi.org/10.1109/icc45041.2023.10279730

Xue, Z., Shang, Y., & Feng, A. (2010). Semi-supervised outlier detection based on fuzzy rough C-means clustering. *Mathematics and Computers in Simulation*, *80*(9), 1911-1921. https://doi.org/10.1016/j.matcom.2010.02.007

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International journal of information security*, *21*(1), 1-44. https://doi.org/10.1007/s10207-021-00545-8

Yeh, C., Choi, Y.-S., Ko, Y.-J., & Kim, I.-G. (2024). Standardization and technology trends of artificial intelligence for mobile systems. *Computer Communications*, *213*(NA), 169-178. https://doi.org/10.1016/j.comcom.2023.11.004

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, *23*(4), 516-539. https://doi.org/10.1080/10439463.2013.780227

Younes, O. (2016). A Secure DHCP Protocol to Mitigate LAN Attacks. *Journal of Computer and Communications*, *04*(1), 39-50. https://doi.org/10.4236/jcc.2016.41005

Younus, M., Hossen, S., & Islam, M. M. (2024). Advanced Business Analytics In Textile & Fashion Industries: Driving Innovation And Sustainable Growth. *International Journal of Management Information Systems and Data Science*, *1*(2), 37-47. https://doi.org/10.62304/ijmisds.v1i2.143

Younus, M., Pathan, S. H., Amin, M. R., Tania, I., & Ouboucetta, R. (2024). Sustainable fashion analytics: predicting the future of eco-friendly textile. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(03), 13-26. https://doi.org/10.62304/jbedpm.v3i03.85

Zhang, Y., Meratnia, N., & Havinga, P. J. M. (2010). Outlier Detection Techniques for Wireless Sensor Networks: A Survey. *IEEE Communications Surveys & Tutorials*, *12*(2), 159-170. https://doi.org/10.1109/surv.2010.021510.00088