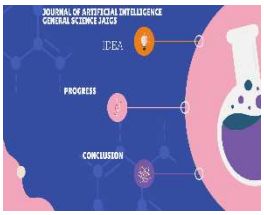
Vol.2,Issue 01, March 2024
Journal of Artificial Intelligence General Science JAIGS



Cyber security Vulnerabilities and Remediation Through Cloud Security Tools

FNU Jimmy

Senior Cloud consultant, Deloitte, USA.

*Corresponding Author:FNU Jimmy

ARTICLEINFO
Article History:
Received:
05.03.2024
Accepted:
10.03.2024
Online: 12.04.2024
Keyword:cyber security; cyber attacks; cyber threats; network security

ABSTRACT

The proliferation of internet usage has surged dramatically, prompting individuals and businesses to conduct myriad transactions online rather than in physical spaces. The onset of the COVID-19 pandemic has further propelled this trend. Consequently, traditional forms of crime have migrated to the digital realm alongside the widespread adoption of digital technologies such as cloud computing, the Internet of Things (IoT), social media, wireless communication, and crypto currencies, amplifying security concerns in cyberspace. Notably, cybercriminals have begun offering cyber attacks as a service, automating attacks to magnify their impact. These attackers exploit vulnerabilities across hardware, software, and communication layers, perpetrating various forms of cyber attacks including distributed denial of service (DDoS), phishing, man-in-the-middle, password, remote, privilege escalation, and malware attacks. The sophistication of these attacks renders conventional protection systems, such as firewalls, intrusion detection systems, antivirus software, and access control lists, ineffective in detection. Consequently, there is an urgent imperative to devise innovative and pragmatic solutions to thwart cyber attacks. This paper elucidates the primary drivers behind cyber attacks, surveys recent attack instances, patterns, and detection methodologies, and explores contemporary technical and non-technical strategies for preemptively identifying and mitigating attacks. Leveraging cutting-edge technologies like machine learning, deep learning, cloud platforms, big data analytics, and blockchain holds promise in combating present and future cyber threats. These technological interventions can aid in malware detection, intrusion detection, spam filtering, DNS attack classification, fraud detection, identification of covert channels, and discernment of advanced persistent threats. Nonetheless, it's crucial to acknowledge that some promising solutions, notably machine learning and deep learning, are susceptible to evasion techniques, necessitating careful consideration when formulating defenses against sophisticated cyber attacks.

Introduction

Introduction

The emergence of the Internet as a global communication and sharing platform has significantly reshaped the landscape of human interaction. Throughout the 21st century, the intertwining of world geography with the Internet network has accelerated, enabling high-speed communication among people worldwide and fostering robust connections between states across various domains such as commerce, politics, economics, and sociocultural spheres. At its core, the Internet comprises three fundamental elements: computers, users, and networks. The evolution of network technologies, propelled by advancements in computer technologies and the diversification of user segments, has ushered in a new era of connectivity and accessibility. However, alongside the rapid development and widespread adoption of network technologies, critical security challenges have arisen.

Efforts have been made to establish a cyber security framework aimed at safeguarding the assets of institutions, organizations, and individuals in the digital realm. The term "cyber" pertains to networks encompassing infrastructure information systems, often referred to as "virtual reality." Cyber security encompasses measures designed to protect the security, integrity, and confidentiality of communication, life, assets, and data within electronic environments established by entities ranging from individuals to large enterprises. In essence, cyber security ensures the safeguarding of virtual life within cyber networks, encompassing the protection of information system infrastructures, data integrity, and confidentiality.

The primary objective of cyber security is to fortify individuals' and institutions' data on the Internet. Neglecting this imperative can expose vulnerabilities through which malicious actors may infiltrate devices over networks and compromise data integrity or pilfer sensitive user credentials such as credit card details or user IDs. Such cyber attacks pose significant financial threats to individuals, organizations, corporations, and even governmental entities. Recent studies indicate that cyber attacks incur billions of dollars in economic losses globally, underscoring the magnitude of this threat. Moreover, contemporary cyber attacks transcend mere isolated incidents, evolving into sophisticated operations backed by significant resources from large corporations and governmental bodies, necessitating robust cyber security policies to mitigate risks effectively.

Against this backdrop, this study endeavors to provide a comprehensive analysis elucidating the fundamentals and significance of cyber security. It delves into all facets of cyber security, presenting shared risks and threats while exploring and evaluating solutions to preemptively mitigate them. The study serves as a guide for researchers in the field, spanning from foundational concepts of cyber and network security to addressing common attack vectors.

To enhance clarity and precision in communication, frequently used phrases and their acronyms are listed in Table 1. This review paper represents, to the best of our knowledge, the most exhaustive examination of cyber security from a multifaceted perspective. Distinguishing itself from previous survey papers, which often focused on specific subjects such as cyber security threats, attacks, blockchain technology implementation, or machine learning techniques in cyber security, this study comprehensively addresses various aspects of cyber security. Each section of the paper meticulously dissects different facets of the cyber security landscape, detailing attack vectors, potential remedies for each class of attack, and associated challenges. While some sections may touch upon similar information, each offers unique insights into the depicted subjects. This paper serves as a valuable resource for researchers and individuals seeking to deepen their understanding of cyber security, spanning from foundational principles to advanced concepts.

Cyber Security Fundamentals

This section delves into the historical context of cyber crime and elucidates the core principles of security. It explores fundamental cyber security solutions and investigates the factors contributing to the surge in cyber attacks. Furthermore, it underscores the pivotal importance of cyber security, examining cyber threats from both technical and non-technical perspectives while proposing actionable measures to mitigate risks.

Threats, Vulnerabilities, Exploits, and Attacks

This segment extensively examines prevalent cyber threats, security vulnerabilities, and attack vectors. It begins by dissecting various cyber threats such as viruses, Trojans, worms, rootkits, and hackers. Subsequently, it delves into known threats like spyware, scareware, joke programs, and ransomware. The discussion then shifts to security vulnerabilities, accompanied by an exploration of commonly utilized vulnerability scanning tools. Finally, a comprehensive analysis

of common attack types—from social engineering attacks to cryptography, hijacking, phishing, malware, bots, and botnets, including password and man-in-the-middle attacks—is provided, alongside recommendations, precautions, and awareness measures for each.

Network Security

This section offers a detailed examination of network security concerns. It begins by elucidating the Open Systems Interconnection (OSI) model, its layers, and associated protocols. Subsequently, it scrutinizes attacks targeting each layer in depth. The discussion then transitions to network protection devices and tools before delving into wireless network security, attacks on wireless networks, and corresponding security methodologies.

The contributions of this study, encompassing detailed discussions on the aforementioned topics, are summarized below:

- Explanation of the current state and shortcomings of the cyber security field alongside technological advancements within this domain.
- Provision of foundational knowledge on cyber security fundamentals.
- Presentation of cyber security risks, threats, attacks, and ongoing research endeavors.
- Examination of network security, OSI layers, and attacks directed at each layer.
- Proposal of existing challenges, issues, and novel assumptions.

With these contributions in mind, this study offers several advantages for researchers in this field:

- Enhanced understanding of the importance of cyber security.
- Accessibility to fundamental concepts for novice researchers.
- Comprehensive insight into prevalent threats and attack types.
- Awareness of current research trends in the cyber security domain.
- Provision of a systematic overview facilitating further study in cyber security.

The subsequent sections of this article are organized as follows: Section 2 provides fundamental insights into cyber security. Section 3 explores prevalent threats, vulnerabilities, exploits, and cyber attacks. Section 4 offers a general overview of network security, while Section 5 discusses cyber security solutions, recommendations, implementation challenges, and avenues for future research. Finally, Section 6 presents the conclusion.

This section provides insights into the history of cyber crime and outlines key security principles. Moreover, it delves into the significance of cyber security, examines the factors contributing to the proliferation of cyber attacks from both technical and non-technical standpoints, and explores potential mitigation strategies.

History of Cyber Crime and Cyber Security

Various terms such as data security, information security, network security, and cyber security have been employed to safeguard digital data. Data security aims to protect digital data throughout its lifecycle, thwarting unauthorized access, modification, or disclosure [14]. Information security, on the other hand, entails preventing unauthorized access, use, disclosure, modification, review, recording, or destruction of physical or electronic information, with a primary focus on safeguarding data confidentiality, integrity, and availability [15]. Network security strives to ensure the confidentiality, integrity, and accessibility of computer networks and transmitted data across communication channels [16]. In contrast, cyber security encompasses the practice of safeguarding computers, servers, mobile devices, electronic systems, computer networks, and data from malicious attacks. While data security, information security, and network security aim to mitigate unauthorized access, use, modification, or destruction of stored or transit data, cyber security encompasses a broader scope, encompassing end-to-end information flows. Presently, the term "cyber security" predominates in usage.

The inception of cyber crime dates back several years, during a time when defending the digital realm was comparatively simpler due to the limited number of machines and less sophisticated attack methodologies. However, technological advancements have empowered cyber criminals to develop automated tools, enabling the execution of increasingly sophisticated cyber attacks. Furthermore, the proliferation of internet-connected devices such as smartphones, tablets, IoT devices, cloud platforms, and social media platforms has expanded the attack surface, catalyzing the evolution of cyber crime from rudimentary exploits to intricate operations that inflict

significant financial losses, amounting to trillions of dollars annually on the global economy [17]. The evolution of cyber crimes over the decades is categorized in Table 2.

Table 1. The classification of cyber crimes over the decades.

Period	Cyber Crimes
1940s	Years without computer crime
1950s	Phone phreaking decade
1960s	Hacking and vulnerability terms appear
1970s	Born of computer security
1980s	The years of ARPANET to Internet
1990s	Computer viruses and worms have become popular
2000s	The Internet grows excessively
2010s	Cyber criminals discover several security breaches in computer systems
2020s	Cyber crimes have become an industry

The emergence of computers in the early 1940s marked a pivotal moment in technological history. However, during this era, devoid of Internet connectivity, computers were utilized in a limited capacity, with no avenues for information sharing between machines. Consequently, the absence of interconnectedness shielded computers from threats and attacks. Phone phreaking emerged in the 1950s as individuals endeavored to exploit phone system protocols to make unauthorized calls or reduce long-distance call charges. Despite efforts by phone companies, mitigating phone phreaking proved challenging. The techniques employed in phone phreaking foreshadowed future tactics utilized in hacking computer systems.

The term "hacking" first surfaced in the 1960s, coinciding with the discovery of the first vulnerability in the IBM 7094 Compatible Time-Sharing System (CTSS) machine in 1965. Subsequently, in 1967, a group of students hired by IBM gained unauthorized access to various system components, illustrating the existence of vulnerabilities within computer systems and laying the groundwork for ethical hacking practices. The genesis of cyber security initiatives can be traced back to the early 1970s with the inception of "The Advanced Research Projects Agency Network" (ARPANET), the precursor to the Internet. In 1971, the creation of the first computer virus, known as the "Creeper," marked a seminal moment in cyber security history. This was followed by the development of the "Reaper," the first antivirus program. In 1979, the arrest of renowned hacker Kevin Mitnick highlighted the emergence of cyber criminal behavior.

The 1980s witnessed a surge in computer-related attacks, primarily perpetrated through computer viruses. This decade also saw the advent of the term "cyber espionage" amid growing concerns about threats from foreign governments. In 1985, the United States Department of Defense (DoD) introduced the "Trusted Computer System Evaluation Criteria" (TCSEC), setting the

foundation for computer security guidelines. The 1986 infiltration of government systems by German hacker Marcus Hess underscored the vulnerabilities within computer networks. Commercial antivirus software was introduced in 1987.

The 1990s witnessed a proliferation of computer systems and the Internet, accompanied by a surge in computer virus prevalence. Notably, macroviruses emerged in 1996, with viruses such as Melissa and ILOVEYOU wreaking havoc worldwide in the late 1990s. Additionally, the introduction of the Secure Sockets Layer (SSL) protocol by Netscape in 1995 enhanced user connections' security over computer networks.

The 2000s witnessed exponential Internet growth and widespread computer usage in both professional and personal domains. However, this increased reliance on computers also amplified security risks, leading to a surge in cyber crime. The emergence of organized hacker groups, coupled with the proliferation of computer worms and Trojans, ushered in new attack methods. The MyDoom worm in 2004 and the Zeus Trojan in 2007 exemplified the evolving landscape of cyber threats, employing distributed denial of service (DDoS) attacks and sophisticated remote access techniques.

In the 2010s, cyber criminals exploited software vulnerabilities and network protocols, resulting in significant financial losses for individuals, corporations, and countries. The Mirai malware in 2016 exploited Internet of Things (IoT) device vulnerabilities to launch DDoS attacks. Ransomware-related attacks, such as WannaCry and LockerGoga, proliferated during this period, causing widespread disruption and financial losses. In 2020, the emergence of CovidLock ransomware underscored the evolving nature of cyber threats, targeting Android devices and denying access to critical data.

The 2020s herald an era where hacking virtually anything in the digital realm is conceivable. Professional websites offering hacking tools as a service have proliferated, facilitating lucrative cyber attacks. Cyber criminals continue to exploit vulnerabilities in hardware, software, and networks, leveraging phishing scams and social engineering techniques. The proliferation of smartphones and IoT devices has expanded attack surfaces, necessitating robust security measures. Fake applications, backdoors, and banking Trojans targeting mobile devices are on the rise, alongside cyber attacks on social media, cryptocurrency, and cloud computing platforms. These evolving cyber threats underscore the critical imperative for continuous vigilance and innovation in cyber security practices.

Table 3. The evolution of cyber attacks over the years [26–31].

Cyber-Related Attack	Year	Attack Spread Method	Consequences
Vladimir Levin's Attack the Citibank1	1994–1995	unknown	around 10 million dollars were stolen
Melissa Virus	1999	used users' trust to click an email attachment	billions of dollars were lost in many countries
ILOVEYOU Worm3	2000	used users' trust to click an email attachment	more than 45 million computers were infected
MyDoom worm4	2004	used attention-grabbing subjects by email, such as errors, tests, etc.	DDoS attacks by allowing remote access was launched
Zeus Trojan	2007	spam email with drive-by downloads	login details such as email and bank accounts were stolen
Stuxnet Worm	2010	attack the programmable logic unit by stealing source codes	control of industrial processes was taken
Attack on USA Natural Gas Pipeline	2012	accessing confidential information through phishing	security credentials were stolen
Mirai Malware	2016	vulnerability of IoT devices was exploited	DDoS attacks were launched
WannaCry Ransomware	2017	windows vulnerability was exploited	computer hard drives were encrypted, and 150 countries were affected
Emotet Trojan	2018	emails in the form of spam and phishing campaigns	sensitive information such as credit card details was stolen
MyFitnessPal	2018	software vulnerability was exploited	150 million users were affected
Ransomware Attack on Magellan	2020	emails in the form of spam and phishing campaigns	health data of 365,000 patients were stolen
CovidLock Ransomware	2020	exploited users' trust by using COVID-19 statistic	android devices' data were encrypted, and data access was denied
Accellion Supply Chain Attack	2021	third-party vulnerabilities were exploited	confidential data from large organizations were stolen
Kaseya Ransomware Attack	2021	zero-day exploits were used	around 1500 companies' data were compromised with the request of 50,000 to 5 million dollar ransoms per victim

Principle of Information Security

Figure 1 delineates the three dimensions of cyber security. The first dimension revolves around safeguarding information from malicious actors, encapsulated within the "principle of information security." This principle embodies the tenets of confidentiality, integrity, and availability (CIA) [35]. The second dimension of cyber security is dedicated to protecting data across all states, encompassing storage, transit [36], and processing. Whether data is transferred between devices via Sneakernet, wired, or wireless networks, cyber security measures must ensure the preservation of data confidentiality, integrity, and availability throughout its journey between network devices and hosts (Figure 1). Finally, the third dimension of cyber security entails leveraging supplementary tools such as policies, practices, new technologies, and user awareness to bolster cyberspace protection.

The principles of information security, namely confidentiality, integrity, and availability, are delineated as follows:

Confidentiality

Confidentiality pertains to shielding information from unauthorized access by users and programs in the digital realm. Data is typically classified into categories such as Top Secret, Secret, Confidential, and Unclassified [37]. Top Secret and Secret data are deemed highly sensitive and necessitate the utmost protection, as their disclosure could pose significant threats to national security. Consequently, access to such data must be rigorously controlled. Similarly, Confidential data holds sensitivity and should be safeguarded against unauthorized disclosure. In contrast, Unclassified data poses minimal sensitivity and is publicly accessible without impacting national security. Hence, governments, organizations, and enterprises must educate their employees on safeguarding valuable assets, including Top Secret, Secret, and Confidential Information, from cyber threats. Encryption, authentication, and access control techniques serve as indispensable measures to uphold data confidentiality.

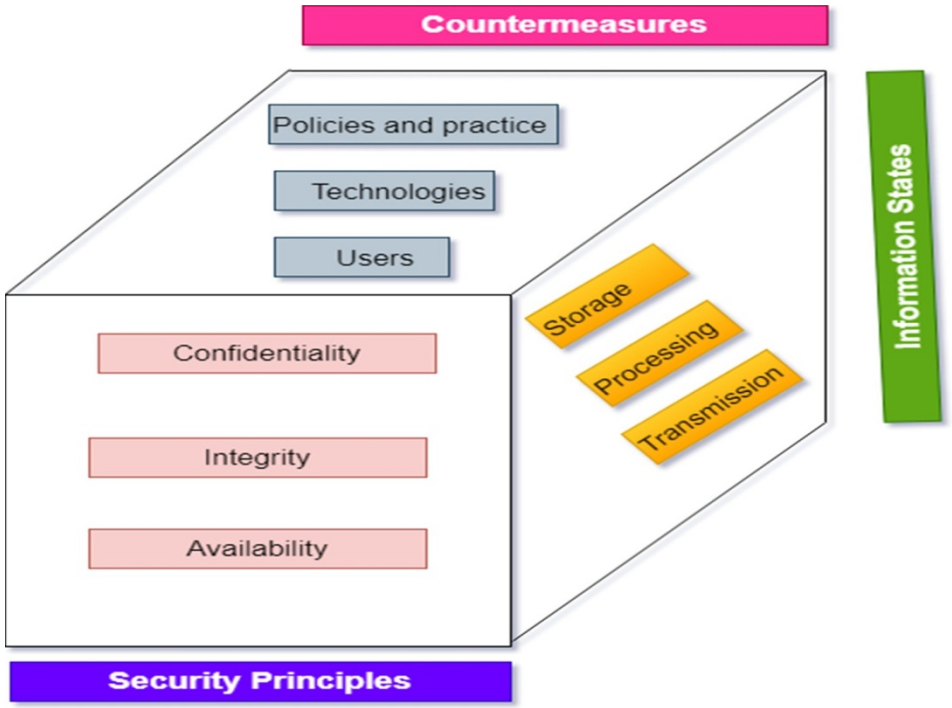


Figure 1: Three Dimensions of Cyber Security

Encryption, a mathematical technique, serves as a pivotal tool in cyber security by transforming original information into an unreadable format, thereby shielding it from unauthorized access [38]. Widely employed in cyber security, encryption plays a crucial role in protecting computer systems and data against brute-force attacks, spyware, and ransomware.

Access control encompasses a range of protective mechanisms designed to thwart unauthorized access to computer systems and networks. As a fundamental security concept, access control plays a paramount role in mitigating risks for organizations.

The AAA concept encompasses three key security services:

1. Authentication: Authentication verifies users' identities through mechanisms such as username-password combinations, thereby preventing unauthorized access [39].

2. Authorization: Authorization determines users' access privileges to computer and network resources, delineating the operations they can undertake [40].

3. Accounting: Accounting monitors users' activities, tracking the resources they access and the changes they enact.

In subsequent sections, we delve into the intricate workings of encryption, authentication, and access control, elucidating their roles in fortifying cyber security measures.

Integrity

Integrity pertains to the accuracy, quality, consistency, and completeness of data throughout its entire lifecycle [41]. Upholding data integrity ensures that information can only be altered by authorized users. Modern enterprises prioritize data integrity for its role in facilitating recoverability, traceability, and connectivity. However, data integrity can be compromised due to various factors such as physical device compromise, disk crashes, malware, hacking, inconsistent

formats, data transfer errors among devices, and human error. To safeguard data integrity, techniques such as hashing, data consistency checks, and data validation checks are employed.

Availability

Availability concerns the accessibility of data, ensuring that authorized users can request or utilize information as needed [43]. System failures and cyber attacks pose threats to information systems and services, potentially impeding data accessibility. DDoS (Distributed Denial of Service) attacks represent a particularly disruptive form of cyber attack that targets a system's availability by overwhelming it with malicious traffic, rendering it inaccessible to legitimate users. While no foolproof solution exists to completely thwart DDoS attacks, ensuring availability necessitates the implementation of strategies such as system backups, redundancy, resiliency, up-to-date operating systems and software, elimination of single points of failure, and prompt detection and response to failures.

Reasons for the Increase in Cyber Attacks

The escalating importance and ubiquity of the Internet globally, coupled with the rapid digitalization of daily life, have fueled the surge in cyber attacks. The COVID-19 pandemic further expedited this digital transformation, with people increasingly relying on online platforms for social interactions, banking, and remote work arrangements (Figure 2). Consequently, traditional crimes have migrated to the digital realm, perpetrated by individuals or organized groups commonly referred to as hackers. Equipped with deep technical knowledge, adept programming skills, and the ability to swiftly identify system vulnerabilities, hackers capitalize on the development of new attack tools and the lucrative economic incentives associated with cyber attacks. Recent studies estimate the staggering economic impact of cyber attacks, amounting to trillions of dollars, with damages steadily rising. Against this backdrop, cyber-related attacks continue to proliferate, exacerbated by factors such as existing system errors, the emergence of new technologies, the dissemination of knowledge, the digitalization of daily life, and the inherent difficulty in detecting attacks that transcend geographical boundaries. Understanding these underlying reasons is crucial for devising effective countermeasures against cyber threats (Figure 2).

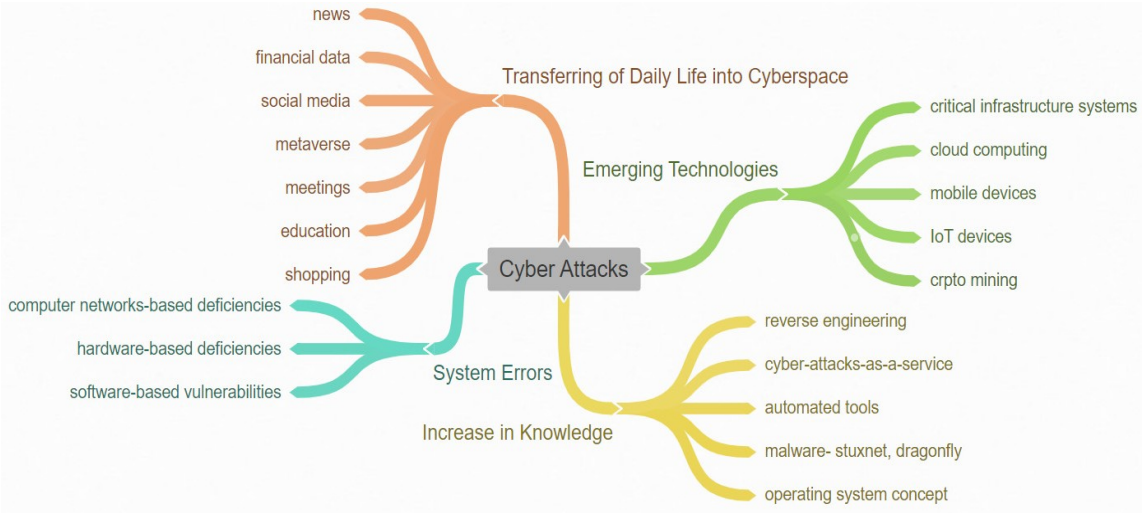


Figure2. Mainreasonsforcyberattacks.

Causes Stemming from Existing System Errors

The surge in cyberattacks can be chiefly attributed to the inherent structure of computer systems and communication networks, rife with vulnerabilities, deficiencies, and misconfigurations in hardware, software, and network protocols, which lay bare these systems to exploitation by hackers. The proliferation of software-based vulnerabilities and protocol deficiencies renders the system susceptible to cyber assaults. Moreover, users' lack of proficiency in navigating the digital landscape and utilizing computer systems compounds the susceptibility to cyber threats. The causes stemming from existing system errors can be categorized into three main groups: attacks triggered by hardware deficiencies, those induced by software-based bugs, and those exploiting vulnerabilities in computer networks.

1. Attacks Caused by Hardware Deficiencies: Attacks originating from hardware flaws and errors pose formidable challenges for detection and prevention, as conventional software-based tools prove inadequate in identifying and mitigating hardware-related attacks [44]. Trojan horses often serve as the primary instigators of hardware attacks, causing resource overconsumption, performance degradation, and system shutdowns by monopolizing excessive power supply [45]. Furthermore, the illicit reproduction of hardware components and procurement of untrustworthy components online pave the way for backdoor entry into computer systems.

The intricate interplay of hardware components and the complexity of integrated circuits render the detection of hardware vulnerabilities exceedingly difficult. A modification in a single integrated circuit can precipitate cascading effects across multiple components, eluding detection

for prolonged periods [46]. Consequently, combating cyberattacks stemming from hardware flaws and errors necessitates robust measures such as tamper-proof hardware devices, hardware watermarking, and obfuscation [47].

2. Attacks Caused by Software-Based Bugs: The majority of cyberattacks continue to be driven by flaws, vulnerabilities, and deficiencies in application software, a trend underscored by the escalating proliferation of software-related vulnerabilities and errors [48,49]. The primary culprits behind software-related vulnerabilities and errors include:

a. Input validation errors

b. Issues with user access control

c. Incomplete or incorrect authentication

d. Directory traversal vulnerabilities

e. Buffer overflow incidents

f. SQL injection vulnerabilities

g. Cross-site scripting (XSS) attacks

h. Usage of components with known vulnerabilities

i. Problems with web services and APIs

j. Inadequate software security testing practices

Despite rapid software development, security testing often falls short during both the development and testing phases, exacerbated by developers' insufficient knowledge of secure software development processes. Additionally, the utilization of applications across diverse platforms and devices introduces vulnerabilities, further exacerbating software-related attacks. For instance, exceeding a buffer's capacity may grant unauthorized access to the system or result in data loss [50]. SQL attacks can overwhelm databases, leading to the theft of sensitive information such as usernames, passwords, and credit card details.

While software updates represent a standard method for rectifying software-related errors and deficiencies, they may not always offer a comprehensive solution. Software updates sometimes inadvertently introduce new issues instead of resolving existing ones. The most effective

approach to mitigating software-based attacks entails cultivating an error-free program design and meticulous requirements analysis before embarking on software code development within the software development lifecycle. Consequently, it is imperative for software developers to undergo training in secure software development processes. Adopting a proactive stance toward security threats and attacks during software development, coupled with rigorous manual and automated testing at every stage, is paramount. Notably, Microsoft's implementation of security development life cycle (SDL) protocols mandated significant reductions in errors and vulnerabilities in the software development process. For instance, the Windows Vista operating system, developed under SDL guidelines, boasts approximately 45% fewer errors and vulnerabilities compared to its predecessor, Windows XP, which was developed without adherence to SDL principles [51].

Causes Stemming from Network Protocol Vulnerabilities

During data transmission across the Internet, hackers can exploit vulnerabilities to access, manipulate, or entirely alter the data. The primary catalyst for such threats lies in the utilization of pre-existing computer network protocols and devices devoid of adequate security measures [44]. Predominantly, attacks against computer networks stem from vulnerabilities within network protocols, including Transmission Control Protocol (TCP), Internet Protocol (IP), Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS). For instance, the absence of a mechanism to ensure the accuracy and confidentiality of packets during their transmission over IP networks renders the information susceptible to exposure and tampering. Similarly, the lack of authentication for DNS responses enables attackers to establish counterfeit servers, potentially leading users to unwittingly connect to these rogue servers instead of legitimate ones. Attackers may also inundate DNS servers with excessive requests, rendering them inaccessible to legitimate users. Furthermore, incomplete or incorrect configurations of network devices, such as switches, routers, and wireless access points, can facilitate data interception during transit.

Efforts to mitigate existing protocol vulnerabilities entail their reduction, the integration of new protocols, and meticulous configuration of network devices to safeguard data traversing computer networks. Commonly employed cybersecurity techniques to mitigate network attacks include:

a. Encryption

b. Access control lists (ACL)

c. Virtualization and Virtual LAN (VLAN)

d. Firewalls

e. Intrusion detection, prevention, and protection systems (IDPS)

f. Web security appliances (WSA)

g. Email security appliances (ESA)

h. Virtual private networks (VPN)

i. Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocols

While these techniques offer a certain degree of data security within the network environment, they do not provide comprehensive protection. Therefore, continuous refinement of these techniques and the proposal of novel approaches remain imperative.

Causes Arising from Emerging Technologies

The rapid advancement of technology introduces novel devices and software into the Internet ecosystem daily, including smartphones, tablets, Internet of Things (IoT) devices, and cloud technology. The proliferation of application programs and the integration of new devices, such as smartphones and IoT devices, into computer networks exacerbate the susceptibility to cyberattacks. Additionally, the consolidation of data from diverse companies onto shared physical infrastructure in the cloud environment, managed and maintained by third parties, raises pertinent security concerns. Key factors precipitating from the evolution of new technologies include:

1. Escalating Smartphone Usage: With approximately 6 billion smartphones in circulation today, nearly half the global population employs smartphones. These devices store personal data, host an expanding array of software applications, and utilize wireless networks for Internet access, rendering them lucrative targets for attackers. Symantec and McAfee cybersecurity threat reports highlight a notable uptick in the creation of malicious software tailored for smartphones. Malware originally designed for traditional computers can be repurposed for smartphone use with minimal modifications.

2. Surging IoT Device Adoption: The proliferation of smart devices, encompassing smart glasses, smartwatches, smart sensors, and automation systems, collectively constituting the

Internet of Things (IoT), is steadily augmenting the Internet landscape. The anticipated proliferation of IoT-connected devices to around 50 billion shortly portends a surge in data traffic, posing challenges in network management. Cyberattacks targeting IoT devices could precipitate substantial data losses, underscoring IoT's emergence as a prominent cyber attack vector.

3. Proliferation of Cloud Computing: Cloud computing, a burgeoning technology that has surged in recent years, caters to user demand by offering scalable, on-demand services. Prominent cloud computing service providers include Amazon, IBM Cloud, Google, Rackspace, Microsoft, and Salesforce. The user-friendly nature, cross-device accessibility, and flexible scalability of cloud services drive their widespread adoption. Additionally, offloading maintenance, repair, and update tasks to cloud service providers bolsters their appeal. However, entrusting third parties with additional privileges engenders security apprehensions in the cloud environment. Key cybersecurity concerns in cloud environments encompass:

a. Loss of control over data by companies and institutions availing cloud services

b. Co-location of data from multiple entities on shared physical infrastructure

c. Security implications associated with data storage in the cloud

d. Vulnerabilities arising from the utilization of virtual machines

e. Cyberattacks during data transit over computer networks

Cloud environments afford users minimal control over data, leading to uncertainties regarding data storage locations and associated security measures. The sharing of physical infrastructure among multiple independent users exposes them to potential data breaches. Additionally, vulnerabilities have been identified in popular virtual machine monitors (VMMs) such as Xen, VMware, and Microsoft Hyper-V, allowing attackers to execute arbitrary code and compromising virtual machine isolation. Consequently, network attacks and vulnerabilities persist as significant threats in the cloud computing milieu. Collaborative efforts between cloud service providers and companies, bolstered by technological and managerial interventions, are imperative to assuage security concerns and fortify data protection in the cloud.

Rise in Critical Infrastructure Systems

Critical infrastructure stands as the backbone of modern society, facilitating uninterrupted daily operations across various sectors. Examples encompass energy production and distribution systems, financial services, communication networks, water and sewer systems, and healthcare

services. Any significant disruption to these systems can profoundly impact society and daily life. Recent studies underscore an alarming surge in both the frequency and severity of cyber attacks targeting critical infrastructure systems. Safeguarding these systems poses formidable challenges owing to their structural intricacy, diverse geographical locations, and the indispensable reliance on the Internet for efficient operation. Key factors driving the escalation of cyber attacks on critical infrastructure systems include:

a. Vulnerabilities stemming from the intricate nature of critical infrastructure systems;

b. Risks arising from the utilization of computer networks during data transmission;

c. Menaces posed by communication protocols employed in SCADA (Supervisory Control and Data Acquisition) systems;

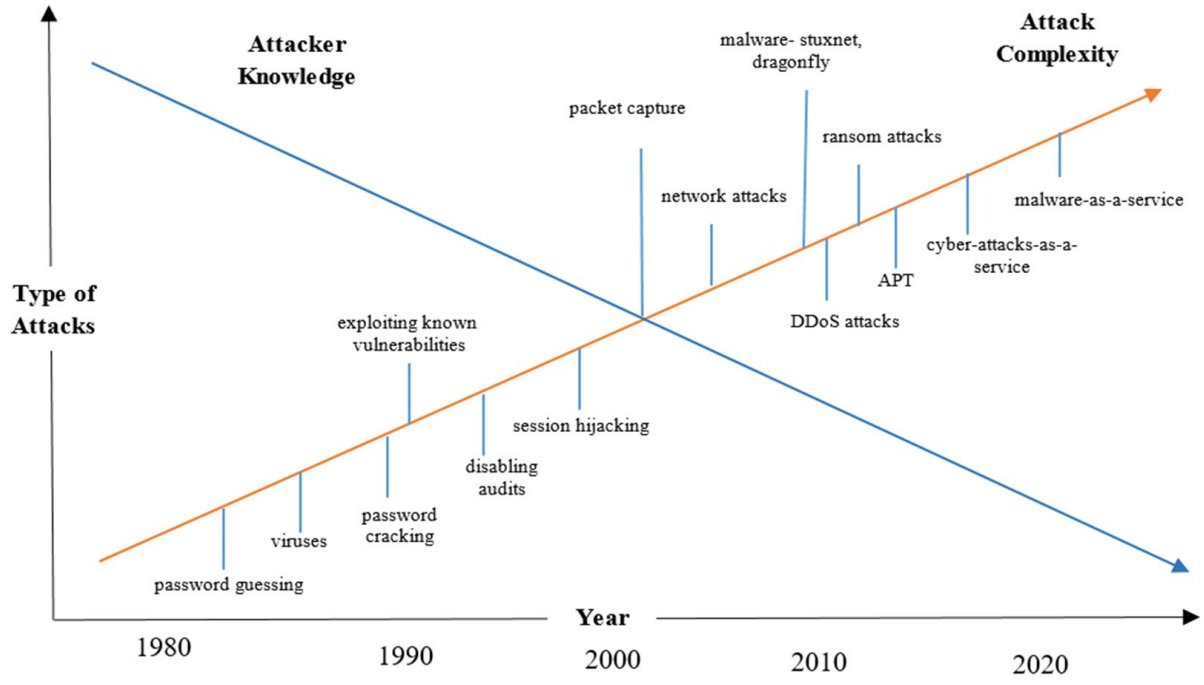
d. Challenges posed by the continuous 24/7 availability of critical infrastructure systems.

The complexity and distinctiveness of critical infrastructure systems entail a multitude of components not found in other systems. This unique structural makeup gives rise to security vulnerabilities absent in conventional setups. Cyber assaults on critical infrastructure systems target various components, including corporate networks, SCADA centers, and remote substations. Any compromise to these elements jeopardizes the entire infrastructure. For instance, an attack on substation sensors can render remote terminal units inoperable or susceptible to external control. Similarly, breaching the SCADA center can grant unauthorized parties control over the entire system. Moreover, communication protocols like Modbus/TCP and DNP3 utilized in SCADA systems are susceptible to numerous attacks. For instance, the absence of encryption in data transmission via these protocols permits unauthorized access and manipulation. Securing critical infrastructure systems presents a formidable challenge owing to their structural complexity, diverse geographical locations, and the indispensable reliance on the Internet for seamless operation.

Reasons Stemming from the Proliferation of Knowledge

The proliferation of knowledge has facilitated the initiation of cyber attacks. In the 1990s and early 2000s, launching attacks on computer systems posed significant challenges. Only seasoned experts with profound expertise in computer systems could execute such attacks. However, in recent years, the accessibility of cyber attack tools, the rapid dissemination of knowledge, and the ease of identifying vulnerabilities in computer software and network protocols have lowered the barriers to launching cyber attacks. Presently, even individuals lacking extensive knowledge about computer systems, commonly referred to as "script kiddies," can carry out attacks using cyber-attack-as-a-service platforms. Many of these platforms are readily accessible on the

Internet. Figure 3 illustrates a comparison between the complexity of attacks and the technical proficiency of attackers. As depicted, although the complexity of attacks has escalated over the years, the level of expertise among attackers has diminished.

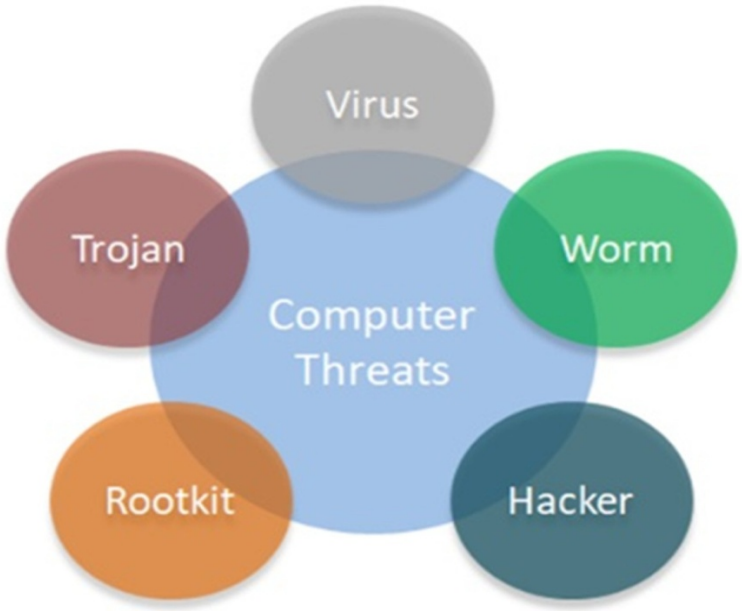


Cyber security Threat Landscape

As the concept of cybersecurity evolves, so does the scope and impact of attacks perpetrated by malicious actors. These attackers target individuals, businesses, and government entities, inflicting significant harm through various means. Among the plethora of attacks, ransomware, phishing, Distributed Denial of Service (DDoS), and mobile threats stand out as prevalent examples. This section delves into the intricacies of cyber threats, delineating security risks, vulnerabilities, and attack vectors in meticulous detail. Additionally, it furnishes recommendations, precautions, and awareness strategies tailored to combat each type of attack.

Threats

A cybersecurity threat pertains to a malevolent entity that illicitly gains entry into computer networks or the networks of individuals or organizations with the intent to cause damage, disruption, or data theft. Below are detailed descriptions of commonly known threat types (refer to Figure 4).



Computer Viruses:

A computer virus is a type of malicious software that alters the normal functioning of a computer system without the user's consent or awareness, often concealing itself within other files. While viruses can operate independently, they typically embed themselves within other programs on a computer. Upon execution, viruses attempt to replicate by spreading to other files. It's worth noting that simply inserting an infected CD, floppy disk, or flash drive into a computer won't infect it unless there's an autorun file prompting execution. Originally, infectious files were limited to program files with extensions such as ".exe," ".com," or ".pif." However, as software technology advanced, the proliferation of executable file types and the evolution of operating systems expanded the scope of potentially harmful file types. For instance, files with ".doc" extensions, once considered simple text files, now accommodate executable programs due to the

development of office software. Similarly, files with ".gif" extensions, typically seen as images, have become potential vectors for viruses by exploiting vulnerabilities in popular operating systems.

Computer Worms:

Worms are a form of malicious software with a more intricate structure than viruses. They are commonly disseminated through email attachments, various websites, and network-shared files. Once infiltrated into a system, worms endeavor to swiftly distribute their source files to other users, leveraging the user's data sources (such as an email address list) without requiring any further action. By proliferating themselves extensively, worms consume users' bandwidth and network resources, potentially causing network crashes, overwhelming email servers, or impeding access to web resources. Unlike viruses, worms don't require user intervention to infect programs; instead, they propagate themselves over a network connection or through downloaded files. To safeguard against worms, installing the latest operating system updates, performing regular system updates, and fortifying defenses against external attacks with personal firewalls are recommended strategies.

Trojan Horses:

Trojan horses are a type of malware that masquerades as legitimate software to lure users into downloading them. Unlike viruses or worms, Trojan horses don't self-replicate. Instead, they rely on user action to execute the program file to which they're attached and proliferate copies. Detecting Trojan horses can be challenging since they don't manifest their effects immediately after infection. Typically, Trojan horses comprise two files: the file sent to the user, which facilitates an attacker's access to the user's computer by opening a port automatically, and the second file, which the attacker runs to gain access. Attackers can exploit these backdoors to pilfer personal information, such as passwords and credit card details, from the victim's system. Moreover, the presence of Trojan horses often enables attackers to install additional malware on the victim's system. Given the diverse nature of Trojan malware, combating them necessitates an extensive defense strategy. Furthermore, regular software updates across all applications, not just the operating system, are vital for reducing system vulnerabilities.

Rootkits:

Rootkits are a category of malware designed to grant hackers unauthorized access to and control over the victim's device. While most rootkits target operating systems and software, some can affect both hardware and software programs. Rootkits excel at concealing their presence and remain active as long as they remain undetected. Upon gaining access to computers, rootkits enable cybercriminals to pilfer financial and personal information, deploy malware, or enlist devices in botnets for circulating spam or executing DDoS attacks. Identifying the files that rootkits have modified, discerning which modules are loaded into the kernel, and determining which network services they might exploit require careful scrutiny. Despite the challenges, certain methods can be employed, such as preserving baseline command outputs and potential infection points to be scrutinized later.

Hackers and Predators:

Computer threats stem from human actions rather than computers themselves. Hackers and predators are individuals who exploit vulnerabilities in computer systems for personal gain or malicious intent. Hackers, in particular, deploy various techniques, such as phishing scams and spam, to disseminate malicious files and compromise security. Employees and users who fail to adhere to safe computer practices can inadvertently pose significant risks to organizational network security. Therefore, ensuring that employees receive proper cybersecurity training is paramount as they constitute the first line of defense against cyberattacks. Without adequate protection, hackers can exploit vulnerabilities to access sensitive information directly, while predators, often concealing their true identities, can compromise personal and financial data. Employing robust firewall solutions and antivirus protection is crucial to thwarting such malicious activities and safeguarding against potential threats.

Risks:

While technological advancements bring about innovation, they also introduce challenges. In response to the demands of the digital era, institutions and organizations store their data in distributed structures across different data centers and cloud environments. However, with corporate and personal data growing increasingly valuable, numerous risks threaten this arrangement at multiple junctures. Furthermore, cyber attackers continually refine their attack methods to exploit computer-based systems more effectively. These activities, spanning scenarios from data theft to ransomware attacks, are collectively termed "Cyber Risks." The following are detailed explanations of the most commonly known types of cyber risks:

Spyware:

Spyware is software that clandestinely collects data without the user's consent or knowledge. It invades privacy by recording keystrokes, monitoring web page views, scanning disk data, and tracking internet searches. This illicit activity may lead to unauthorized actions, such as stealing email and bank passwords, generating intrusive pop-up ads, spamming, and consuming network and system resources, which can degrade web browsing speed or cause general computer slowdown. Unlike viruses, spyware typically doesn't cause direct harm to the user and is often installed with the user's consent or as a result of their actions, albeit without full disclosure of its activities. To safeguard against spyware, security measures such as avoiding downloads from untrusted sources, refraining from connecting unverified devices, and exercising caution with unknown emails are essential.

Scareware:

Scareware belongs to the category of malicious software known as "Rogueware." It employs unrealistic scenarios to intimidate users into purchasing purportedly protective software. Upon installation, however, the scareware exacerbates the situation by infecting the device with a virus, preventing access to computer data. Scareware's primary objective is to generate revenue

for its proprietor. Often, users encounter pop-up messages upon visiting websites, falsely claiming the presence of threats on their computers. These pop-ups not only assert the existence of viruses but also peddle scareware software as the solution. The overarching aim is to exploit users' fears and coerce them into purchasing the software. While scareware can be deleted through the Program, Add/Remove menu of the computer, panic is unwarranted, as it typically doesn't inflict permanent damage.

Joke Programs:

Joke programs are benign applications designed primarily for entertainment or annoyance. Although they're typically harmless, some users may inadvertently engage in actions that could compromise data integrity, such as formatting drives or deleting files. While joke programs may temporarily disable devices like mice or printers, they generally don't inflict lasting harm to other programs, systems, or data. However, they can prove costly for institutions or organizations.

Ransomware:

Ransomware stands out as one of the most prevalent cyber risks, rendering critical files, documents, applications, operating systems, networks, or servers inaccessible. This form of malware encrypts all files and documents on the network, including servers, from a single computer. Upon infection, victims are often extorted to pay a ransom in cryptocurrency in exchange for the promise of data restoration. However, even after ransom payment and file decryption, there's no guarantee that criminals haven't retained copies of the data, leaving room for fraudulent or phishing attempts. Ransomware typically infiltrates systems through deceptive attachments or links in emails purporting to be from reputable entities. Downloading or attempting to open such files is sufficient to trigger ransomware infection.

Hacking Tools:

Hacking entails the intentional modification of computer software or hardware beyond their intended boundaries and design. Hacking tools are programs or utilities crafted to facilitate hacking activities. While some hacking tools may serve proactive purposes, like protecting networks or computers from hackers, others are designed to infiltrate systems. For instance, Hacktool: Win32/Keygen is a well-known hacking tool capable of generating counterfeit activation keys or licenses for various software. Although the tool itself isn't inherently malicious, it's often bundled with malware. Consequently, users who inadvertently install Hacktool: Win32/Keygen may find their computers infected. Many hacking tools are utilized to gain unauthorized access to computers and introduce worms, viruses, or Trojans, leading to severe consequences such as data loss, personal account hijacking, and identity or savings theft.

Remote Access:

Remote access applications enable users to connect to and manage their computers over the internet from any location, operating over specific protocols. While seemingly convenient, remote access poses significant risks, as many individuals, institutions, and organizations fail to secure remote connection services adequately. Attackers exploit vulnerabilities in computer or network security software to gain unauthorized access to machines or systems. Remote access

attacks aim to illegally view or steal data, introduce viruses or other malware, or inflict damage on targeted computers or networks. Other attacks facilitated via remote access include email phishing, third-party provider compromise, insider threats, social engineering, and exploiting vulnerable applications to compromise systems. To guard against remote access attacks, it's crucial to avoid using VPNs with outdated or insecure protocols and to mandate multifactor authentication for each VPN account. Additionally, applying at least two layers of security before permitting remote device management and installing and updating antivirus and antimalware programs are essential protective measures.

Vulnerabilities:

A vulnerability refers to a flaw within a product or system that could potentially allow an attacker to compromise the confidentiality, integrity, or availability of that product or system. Here's a brief overview of various types of vulnerabilities:

Software vulnerabilities: These arise when applications contain errors or bugs, providing attackers with an opportunity to exploit these weaknesses and compromise the system. Examples include buffer overflow and race conditions.

Firewall vulnerabilities: Firewalls act as safeguards, protecting networks from attacks. Vulnerabilities in firewalls stem from errors or deficiencies in their design, implementation, or configuration, which attackers can exploit to launch attacks against the trusted network they are intended to protect.

TCP/IP vulnerabilities: Vulnerabilities in these protocols, spanning various layers of a network, may lack desired features in an unsecured network, making them susceptible to attacks such as ARP attacks and fragmentation attacks.

Wireless network vulnerabilities: Wireless LANs face protocol-based attacks similar to wired LANs, and insecure wireless access points can pose a threat by providing unauthorized entry points to personal or corporate networks. Examples include vulnerabilities related to the Service Set Identifier (SSID) and Wired Equivalent Privacy (WEP) issues.

Operating system vulnerabilities: Security vulnerabilities in operating systems like Windows, macOS, and Unix can compromise the security of the applications running on them. Negligence by system administrators can leave operating systems vulnerable to exploitation.

Web server vulnerabilities: These vulnerabilities result from design flaws or misapplications, leading to attacks such as sniffing and spoofing.

Vulnerability Scanning Tools:

Vulnerability scanning tools are essential for detecting security vulnerabilities in devices and software systems. They rely on vulnerability databases to identify specific vulnerabilities and provide warnings or reports. Here are some widely used vulnerability scanning tools:

Netsparker: An accurate, automatic scanner for identifying vulnerabilities in web applications and APIs. It confirms vulnerabilities and distinguishes them from false positives, saving time during scans.

Acunetix: A fully automated web vulnerability scanner capable of detecting over 4500 web application vulnerabilities, including SQL Injections and XSS. It provides comprehensive reports and supports single-page applications with HTML5 and JavaScript.

Intruder: An advanced vulnerability scanner that conducts proactive scans for newly released vulnerabilities. It integrates with Slack and Jira for real-time updates and offers AWS integration for IP address synchronization.

SolarWinds Network Configuration Manager: Offers network vulnerability detection capabilities, monitoring, managing, and safeguarding network configurations. It provides notifications for configuration changes and enables configuration backup.

Apptrana: A web application vulnerability scanner that automates detection and reporting of security vulnerabilities. It offers proof-of-concept requests for validation and integration with Indusface WAF for virtual patching.

OpenVAS: An open-source tool for centralized vulnerability scanning and management. It features a regularly updated scan engine and is compatible with various operating systems.

Nexpose Community: Developed by Rapid7, it performs network checks and vulnerability scans, prioritizing security vulnerabilities based on various factors. It automatically identifies and scans new devices, integrating with the Metasploit framework.

Nikto: A widely used open-source web scanner for evaluating potential web server vulnerabilities. It conducts thorough tests on web servers, scanning multiple protocols such as HTTP, HTTPS, and HTTPD.

Evaluation of Cyber Security Vulnerabilities, Threats, Attacks, Solutions, and Future Challenges

This section delves into cyber security threats, attacks, potential solutions, and future research directions. Figure 9 illustrates the security solutions implemented in the cyber security domain, categorized into technical and non-technical solutions.

Non-technical solutions encompass physical and administrative aspects. Physical security entails safeguarding areas, securing computing devices, implementing data center disaster recovery plans, and strategically locating backups. Administrative measures involve management strategies such as policies, procedures, standards, risk assessments, vendor management, assigned responsibilities, and training. Adequate training of system users is crucial, as even the most robust protection system crafted by cyber security specialists may fall short without user proficiency.

Technical solutions fall into three primary groups: technologies and platforms, utilized tools, and the integration of AI and data science. Figure 9 highlights key technologies and platforms. Cryptography ensures data integrity and confidentiality during storage and transit. Access control restricts data access, enhancing security and reducing vulnerability to remote attacks and privilege escalation. Big data facilitates the analysis of vast datasets to uncover unknown patterns and identify malicious attack characteristics.

Emerging technologies such as blockchain, virtualization, and big data are increasingly applied in cyber security. Blockchain validates data consistency and detects complex attacks. Virtualization separates software applications from hardware components, enhancing usability, reducing costs, and minimizing downtime during cyber attacks. Cloud computing platforms offer proactive threat management, advanced data security, scalability, high availability, and efficient data recovery.

Numerous well-established tools and protocols aid in detecting, preventing, and mitigating attacks. Access control lists (ACLs) and firewalls filter packets based on predefined rules, reducing DDoS attacks. Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) detect intrusions using signatures or anomalies in computer networks. Virtual private networks (VPNs), IPsec, TLS, and SSL technologies protect data confidentiality and integrity during network transmission. Web security appliances (WSAs) and email security appliances (ESAs) safeguard web and email servers, respectively. Antivirus scanners identify malware-related attacks on end hosts, while vulnerability scanners detect and classify system vulnerabilities, enabling timely patching.

To effectively protect computer systems, a comprehensive approach incorporating all aforementioned tools, protocols, and technologies (Figure 9) across each layer is imperative. Additionally, the development of new attack detection systems utilizing statistics, probability, data mining, and machine learning techniques is essential to stay ahead of evolving cyber threats.

The landscape of attacks and defense strategies is constantly evolving, rendering current detection systems less effective over time. To address this challenge, new solutions can be integrated into existing frameworks or entirely new systems can be developed to counter more

sophisticated attacks. In this context, statistics, probability, data mining, and machine learning techniques play crucial roles.

Statistics, as a scientific method, analyzes and interprets data to unveil patterns. Probability assesses the likelihood of events occurring. Data mining uncovers hidden patterns in large datasets and intersects with statistics, machine learning, and computer science. Machine learning techniques enable computers to learn from data without explicit programming, algorithmically describing the data.

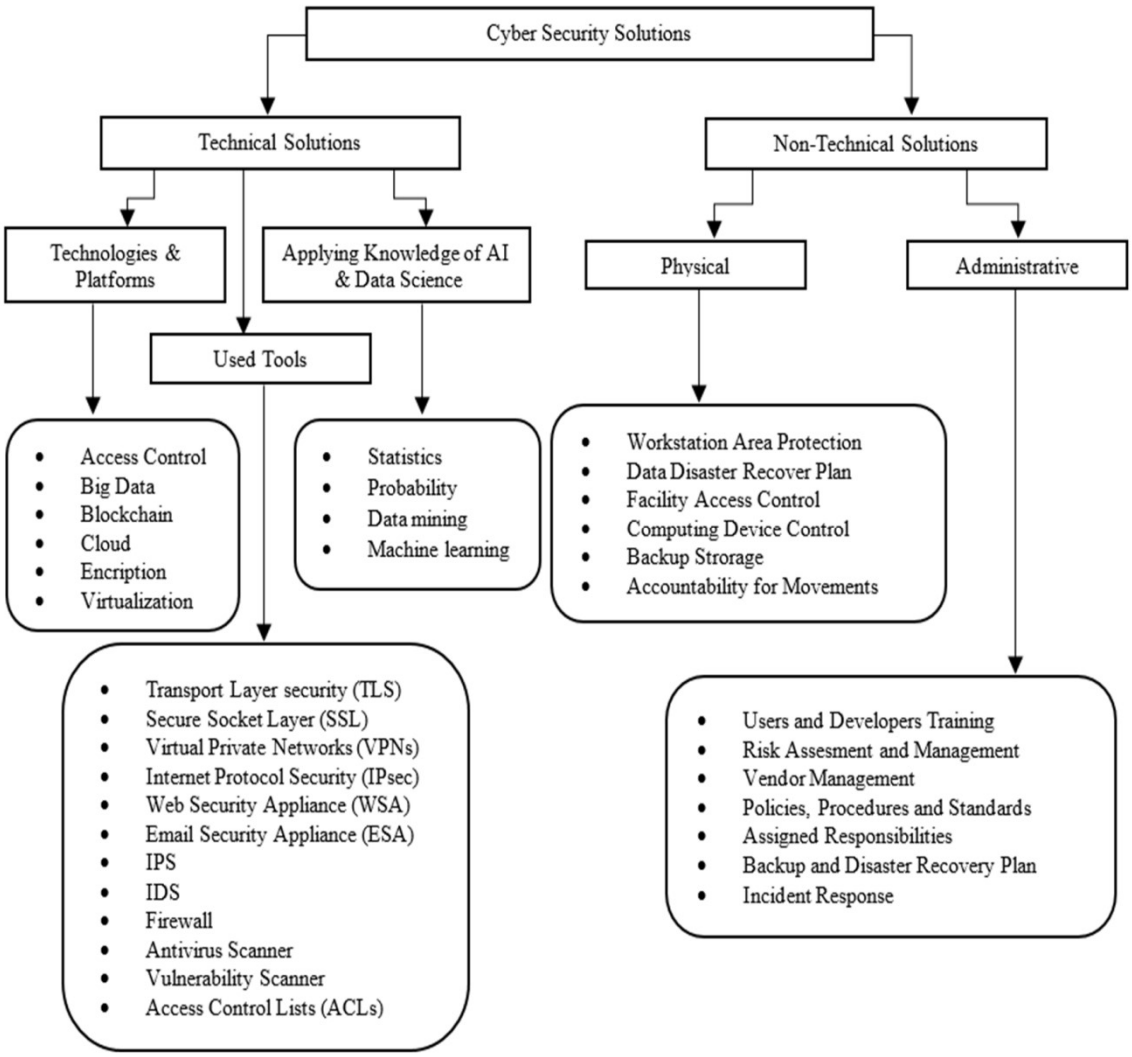
While statistics and probability-based solutions have long been utilized in cyber security, data mining and machine learning techniques have gained prominence in recent years. These innovative technologies enhance existing attack detection systems by introducing new features and intelligence to combat evolving cyber threats.

Machine learning encompasses a diverse range of techniques, including regression, probabilistic models, distance-based learning, decision trees, dimensionality reduction algorithms, and boosting-bagging algorithms, all applicable in cyber security. These techniques enable the scanning of data breaches and vulnerabilities in computer systems and communication networks, providing rapid analysis of large datasets and adaptation without expert intervention. Moreover, machine learning methods significantly improve threat detection accuracy and optimize network efficiency using heuristic approaches.

Machine learning techniques find application across various domains within cyberspace, including:

- Malware detection
- Spam identification
- Fraud detection
- Detection of malicious JavaScript
- Anomaly detection
- Classification of malware
- Risk assessment
- DNS classification
- Phishing detection
- Leakage detection
- Detection of hidden channels
- Botnet detection
- Detection of Distributed Denial of Service (DDoS) attacks
- Zero-day threat detection
- Detection of Advanced Persistent Threats (APTs)
- Identification of social media attacks
- Vulnerability detection
- Detection of cryptographic attacks

By leveraging machine learning in these areas, cyber security professionals can enhance their defense mechanisms and stay ahead of emerging threats.



Representthetechnicalandnon-technicalcybersecuritysolutions.

Despite numerous advancements in detecting cyber attacks, significant challenges persist in the field of cyber security. These challenges include:

1. Time-consuming process of designing a secure system

2. Difficulty in creating, storing, and distributing confidential information
3. Security often being considered an afterthought
4. Perception of security as a barrier
5. Burden on security professionals to identify and fix all vulnerabilities, while attackers need only find one
6. Transformation of security into a human issue
7. Complexity in detecting and preventing unknown attacks
8. Increasing complexity of attacks
9. Automation of attacks through cyber-attacks-as-a-service
10. Evasion of detection systems by intelligent attacks
11. Assumption of data by machine learning (ML)-based algorithms
12. Proneness of ML-based algorithms to bias
13. Inability of ML-based algorithms to handle outliers consistently
14. Rise in ML-based attacks
15. Difficulty in classifying millions of network connections
16. Handling of high-dimensional data
17. Complexity of data preprocessing due to multiple data formats
18. Challenges in creating contextual features
19. Difficulty in applying domain knowledge for automated analysis
20. Limited availability of consistent and up-to-date datasets for testing proposed methods in cyber security
21. Complexity of protecting multiple components
22. Complexity of the attack vector
23. Insider attacks
24. Use of outdated hardware
25. Increasing software vulnerabilities
26. Risk of losing control over data
27. Rise in cloud-based attacks
28. Expansion of Internet of Things (IoT)-based threats
29. Increasing complexity of ransomware attacks
30. Evolution of social engineering techniques

Addressing these challenges requires concerted efforts from both researchers and practitioners in the cyber security domain.

conclusion

In conclusion, this comprehensive review paper provides insights into cyber security issues and solutions based on recent technological advancements. We have segmented cyber security topics into three main sections: cyber security fundamentals, threats, vulnerabilities, exploits, and attacks, and network security at various levels. This segmentation is crucial for a thorough understanding of cyber security components and for devising holistic solutions to security challenges.

The section on cyber security fundamentals outlines both technical and nontechnical factors contributing to the rise of cyber attacks. These attacks are dynamic and constantly evolving, impacting all computer-based systems and the online environment. Social life's migration to the digital realm further amplifies cyber threats, exacerbated by software errors, network protocol vulnerabilities, increasing device connectivity, and the complexity of critical systems. Additionally, factors such as the virtualization of social interactions, extensive use of social media, heightened attacker knowledge, and user negligence in online activities elevate security risks in the digital landscape.

The threats, vulnerabilities, exploits, and attacks section delves into the core components of attack strategies exploiting system and third-party software vulnerabilities. Cyber attackers deploy sophisticated malicious code blocks to exploit vulnerabilities in computer-based systems. Common threats include malware (viruses, worms, rootkits, ransomware), hacking tools, application attacks, access attacks, cryptography attacks, and Advanced Persistent Threats (APTs). The emergence of cyber-attacks-as-a-service tools has further escalated the frequency of attacks, posing challenges to detection processes.

Each layer of network security is thoroughly examined, outlining common attacks and potential solutions. Attacks often target specific layer protocols to succeed, categorized as physical-layer attacks (e.g., sniffing), data-link-layer attacks (e.g., MAC spoofing), and so forth. Vulnerabilities in network protocols and misconfigured network devices contribute to attack success. Addressing these vulnerabilities requires reducing existing protocol vulnerabilities, introducing new protocols, and ensuring proper configuration of network devices to safeguard data traversing computer networks.

Effective protection against cyber threats necessitates collaboration among individuals, organizations, software developers, and governments. Solutions can be broadly categorized into technical and nontechnical measures. Nontechnical solutions encompass administrative-based management, policies, standards, procedures, risk assessment, vendor management, assigned responsibilities, and training to ensure user competence. Meanwhile, technical solutions leverage technological advancements and scientific principles to create intelligent applications for combating attackers. These solutions encompass cryptography, access control, big data analytics, virtualization, cloud computing, blockchain technology, statistical methods, data mining, and machine learning (ML) techniques.

While technological advancements significantly enhance the ability to detect and mitigate cyber threats, challenges persist in effectively combating new and complex attacks. These challenges include the increasing complexity and automation of attacks, evasion of detection systems by intelligent attackers, biases in ML-based algorithms, classification of vast network connections, handling high-dimensional data, safeguarding multiple components, and addressing the human

aspect of security.

In conclusion, the cyber security landscape is evolving rapidly, necessitating continuous innovation and collaboration to stay ahead of emerging threats and vulnerabilities. Addressing these challenges requires a multifaceted approach encompassing both technical innovations and robust nontechnical strategies.

References:

[1]. Rehan, H. (2024). Revolutionizing America's Cloud Computing the Pivotal Role of AI in Driving Innovation and Security. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 189-208. DOI: https://doi.org/10.60087/jaigs.v2i1.p208

[2]. Rehan, H. (2024). AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 47-66. DOI: https://doi.org/10.60087/jaigs.v1i1.p66

[3]. Islam, M. M. (2024). Exploring Ethical Dimensions in AI: Navigating Bias and Fairness in the Field. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 13-17.**DOI:** https://doi.org/10.60087/jaigs.v1i1.p18

[4]. Khan, M. R. (2024). Advances in Architectures for Deep Learning: A Thorough Examination of Present Trends. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 24-30. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p30

[5]. Shuford, J., & Islam, M. M. (2024). Exploring the Latest Trends in Artificial Intelligence Technology: A Comprehensive Review. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1). **DOI:** https://doi.org/10.60087/jaigs.v2i1.p13

[6]. Islam, M. M. (2024). Exploring the Applications of Artificial Intelligence across Various Industries. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 20-25.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p25

[7]. Akter, S. (2024). Investigating State-of-the-Art Frontiers in Artificial Intelligence: A Synopsis of Trends and Innovations. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 25-30.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p30

[8]. Rana, S. (2024). Exploring the Advancements and Ramifications of Artificial Intelligence. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 30-35.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p35

[9]. Sarker, M. (2024). Revolutionizing Healthcare: The Role of Machine Learning in the Health Sector. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 35-48.

DOI: https://doi.org/10.60087/jaigs.v2i1.p47

[10]. Akter, S. (2024). Harnessing Technology for Environmental Sustainability: Utilizing AI to Tackle Global Ecological Challenges. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 49-57.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p57

[11]. Padmanaban, H. (2024). Revolutionizing Regulatory Reporting through AI/ML: Approaches for Enhanced Compliance and Efficiency. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 57-69.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p69

[12]. Padmanaban, H. (2024). Navigating the Role of Reference Data in Financial Data Analysis: Addressing Challenges and Seizing Opportunities. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 69-78.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p78

[13]. Camacho, N. G. (2024). Unlocking the Potential of AI/ML in DevSecOps: Effective Strategies and Optimal Practices. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 79-89.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p89

[14]. PC, H. P., & Sharma, Y. K. (2024). Developing a Cognitive Learning and Intelligent Data Analysis-Based Framework for Early Disease Detection and Prevention in Younger Adults with Fatigue. *Optimized Predictive Models in Health Care Using Machine Learning*, 273.

[15]. Padmanaban, H. (2024). Quantum Computing and AI in the Cloud. *Journal of Computational Intelligence and Robotics*, *4*(1), 14–32. Retrieved from https://thesciencebrigade.com/jcir/article/view/116

[18]. Harish Padmanaban, P. C., & Sharma, Y. K. (2024). Optimizing the Identification and Utilization of Open Parking Spaces Through Advanced Machine Learning. *Advances in Aerial Sensing and Imaging*, 267-294. **https://doi.org/10.1002/9781394175512.ch12**

[19]. PC, H. P., Mohammed, A., & RAHIM, N. A. (2023). *U.S. Patent No. 11,762,755*. Washington, DC: U.S. Patent and Trademark Office.https://patents.google.com/patent/US20230385176A1/en

[20]. Padmanaban, H. (2023). Navigating the intricacies of regulations: Leveraging AI/ML for Accurate Reporting. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3), 401-412.DOI: https://doi.org/10.60087/jklst.vol2.n3.p412

[21]. PC, H. P. Compare and analysis of existing software development lifecycle models to develop a new model using computational intelligence.https://shodhganga.inflibnet.ac.in/handle/10603/487443

[22]. Latif, M. A., Afshan, N., Mushtaq, Z., Khan, N. A., Irfan, M., Nowakowski, G., ... &Telenyk, S. (2023). Enhanced classification of coffee leaf biotic stress by synergizing feature concatenation and dimensionality reduction. *IEEE Access*.
DOI: https://doi.org/10.1109/ACCESS.2023.3314590

[23]. Irfan, M., Mushtaq, Z., Khan, N. A., Mursal, S. N. F., Rahman, S., Magzoub, M. A., ... & Abbas, G. (2023). A Scalo gram-based CNN ensemble method with density-aware smote oversampling for improving bearing fault diagnosis. *IEEE Access*, *11*, 127783-127799.
DOI: https://doi.org/10.1109/ACCESS.2023.3332243

[24]. Irfan, M., Mushtaq, Z., Khan, N. A., Althobiani, F., Mursal, S. N. F., Rahman, S., ... & Khan, I. (2023). Improving Bearing Fault Identification by Using Novel Hybrid Involution-Convolution Feature Extraction with Adversarial Noise Injection in Conditional GANs. *IEEE Access*.

DOI: https://doi.org/10.1109/ACCESS.2023.3326367

[25]. Rahman, S., Mursal, S. N. F., Latif, M. A., Mushtaq, Z., Irfan, M., & Waqar, A. (2023, November). Enhancing Network Intrusion Detection Using Effective Stacking of Ensemble Classifiers With Multi-Pronged Feature Selection Technique. In *2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)* (pp. 1-6). IEEE.

DOI: https://doi.org/10.1109/ETECTE59617.2023.10396717

[26]. Latif, M. A., Mushtaq, Z., Arif, S., Rehman, S., Qureshi, M. F., Samee, N. A., ... & Al-masni, M. A. Improving Thyroid Disorder Diagnosis via Ensemble Stacking and Bidirectional Feature Selection.
https://doi.org/10.32604/cmc.2024.047621

[32]. Zhu, M., Zhang, Y., Gong, Y., Xing, K., Yan, X., & Song, J. (2024). Ensemble Methodology: Innovations in Credit Default Prediction Using LightGBM, XGBoost, and LocalEnsemble. *arXiv preprint arXiv:2402.17979*.

https://doi.org/10.48550/arXiv.2402.17979

[33]. Yafei, X., Wu, Y., Song, J., Gong, Y., &Lianga, P. (2024). Generative AI in Industrial Revolution: A Comprehensive Research on Transformations, Challenges, and Future Directions. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *3*(2), 11-20.

DOI: https://doi.org/10.60087/jklst.vol.3n2.p20

[34]. Xu, J., Wang, H., Zhong, Y., Qin, L., & Cheng, Q. (2024). Predict and Optimize Financial Services Risk Using AI-driven Technology. *Academic Journal of Science and Technology*, *10*(1), 299-304.

https://drpress.org/ojs/index.php/ajst/article/view/19205

[41]. Pillai, A. S. (2023). Advancements in Natural Language Processing for Automotive Virtual Assistants Enhancing User Experience and Safety. *Journal of Computational Intelligence and Robotics*, *3*(1), 27-36.

https://thesciencebrigade.com/jcir/article/view/161

[42]. Sharma, Y. K., & Harish, P. (2018). Critical study of software models used cloud application development. *International Journal of Engineering & Technology, E-ISSN*, 514-518.

https://scholar.google.com/citations?view_op=view_citation&hl=en&user=Fxv3elcAAAAJ&citation_for_view=Fxv3elcAAAAJ:d1gkVwhDpl0C

[43]. PC, H. P., Mohammed, A., & RAHIM, N. A. (2023). *U.S. Patent No. 11,762,755*. Washington, DC: U.S. Patent and Trademark Office.

https://patents.google.com/patent/US11762755B2/en

[44]. Miah, S., Rahaman, M. H., Saha, S., Khan, M. A. T., Islam, M. A., Islam, M. N., ... & Ahsan, M. H. (2013). Study of the internal structure of electronic components RAM DDR-2 and motherboard of nokia-3120 by using neutron radiography technique. *International Journal of Modern Engineering Research (IJMER)*, *3*(60), 3429-3432

[45]. Rahaman, M. H., Faruque, S. B., Khan, M. A. T., Miah, S., & Islam, M. A. (2013). Comparison of General Relativity and Brans-Dicke Theory using Gravitomagnetic clock effect. *International Journal of Modern Engineering Research*, *3*, 3517-3520.

[46]. Miah, M. H., & Miah, S. (2015). The Investigation of the Effects of Blackberry Dye as a Sensitizer in TiO2 Nano Particle Based Dye Sensitized Solar Cell. *Asian Journal of Applied Sciences*, *3*(4).

[48]. Miah, S., Miah, M. H., Hossain, M. S., & Ahsan, M. H. (2018). Study of the Homogeneity of Glass Fiber Reinforced Polymer Composite by using Neutron Radiography. *Am. J. Constr. Build. Mater*, *2*, 22-28.

[49]. Miah, S., Islam, G. J., Das, S. K., Islam, S., Islam, M., & Islam, K. K. (2019). Internet of Things (IoT) based automatic electrical energy meter billing system. *IOSR Journal of Electronics and Communication Engineering*, *14*(4 (I)), 39-50.

[50]. Nadia, A., Hossain, M. S., Hasan, M. M., Islam, K. Z., & Miah, S. (2021). Quantifying TRM by modified DCQ load flow method. *European Journal of Electrical Engineering*, *23*(2), 157-163.

[51]. Miah, S., Raihan, S. R., Sagor, M. M. H., Hasan, M. M., Talukdar, D., Sajib, S., ... &Suaiba, U. (2022). Rooftop Garden and Lighting Automation by the Internet of Things (IoT). *European Journal of Engineering and Technology Research*, *7*(1), 37-43.

DOI: https://doi.org/10.24018/ejeng.2022.7.1.2700

[52]. Prasad, A. B., Singh, S., Miah, S., Singh, A., & Gonzales-Yanac, T. A Comparative Study on Effects of Work Culture on employee satisfaction in Public & Private Sector Bank with special reference to SBI and ICICI Bank.

[53]. Ravichandra, T. (2022). A Study On Women Empowerment Of Self-Help Group With Reference To Indian Context.

https://www.webology.org/data-cms/articles/20220203075142pmwebology%2019%20(1)%20-%2053.pdf

[54]. Kumar, H., Aoudni, Y., Ortiz, G. G. R., Jindal, L., Miah, S., & Tripathi, R. (2022). Light weighted CNN model to detect DDoS attack over distributed scenario. *Security and Communication Networks*, *2022*.

https://doi.org/10.1155/2022/7585457

[55]. Ma, R., Kareem, S. W., Kalra, A., Doewes, R. I., Kumar, P., & Miah, S. (2022). Optimization of electric automation control model based on artificial intelligence algorithm. *Wireless Communications and Mobile Computing*, *2022*.

https://doi.org/10.1155/2022/7762493

[56]. Devi, O. R., Webber, J., Mehbodniya, A., Chaitanya, M., Jawarkar, P. S., Soni, M., & Miah, S. (2022). The Future Development Direction of Cloud-Associated Edge-Computing Security in the Era of 5G as Edge Intelligence. *Scientific Programming*, *2022*.

https://doi.org/10.1155/2022/1473901

[57]. Al Noman, M. A., Zhai, L., Almukhtar, F. H., Rahaman, M. F., Omarov, B., Ray, S., ... & Wang, C. (2023). A computer vision-based lane detection technique using gradient threshold and hue-lightness-saturation value for an autonomous vehicle. *International Journal of Electrical and Computer Engineering*, *13*(1), 347.

https://shorturl.at/ceoyJ

[58]. Patidar, M., Shrivastava, A., Miah, S., Kumar, Y., &Sivaraman, A. K. (2022). An energy efficient high-speed quantum-dot based full adder design and parity gate for nano application. *Materials Today: Proceedings*, *62*, 4880-4890.

https://doi.org/10.1016/j.matpr.2022.03.532

[59]. Gitte, M., Bawaskar, H., Sethi, S., & Shinde, A. (2014). Content based video retrieval system. *International Journal of Research in Engineering and Technology*, *3*(06), 123-129.https://scholar.google.co.in/citations?view_op=view_citation&hl=en&user=XlLBRR4AAAAJ&citation_for_view=XlLBRR4AAAAJ:u5HHmVD_uO8C

[60]. Shivakumar, S. K., &Sethii, S. (2019). *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*. Apress.

[61]. Sethi, S., & Panda, S. (2024). Transforming Digital Experiences: The Evolution of Digital Experience Platforms (DXPs) from Monoliths to Microservices: A Practical Guide. *Journal of Computer and Communications*, *12*(2), 142-155.

DOI: https://doi.org/10.4236/jcc.2024.122009

[62]. Sethi, S. (2018). Healthcare blockchain leads to transform healthcare industry. *International Journal of Advance Research, Ideas and Innovations in Technology*, *4*(1), 607-608.

[62]. Sethi, S., &Shivakumar, S. K. (2023). DXPs Digital Experience Platforms Transforming Fintech Applications: Revolutionizing Customer Engagement and Financial Services. *International Journal of Advance Research, Ideas and Innovations in Technology*, *9*, 419-423.

[63]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., &Sethii, S. (2019). DXP Security. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 183-200.

DOI https://doi.org/10.1007/978-1-4842-4303-9_6

[64]. Sethi, S., & Panda, S. (2023). The Evolution of Monolithic DXPs to Microservice based DXPs. *Authorea Preprints*.

DOI https://doi.org/10.36227/techrxiv.24328504.v1

[65]. Sethi, S., Panda, S., &Kamuru, R. (2023). Comparative study of middle tier caching solution. *International Journal of Development Research*, *13*(11), 64225-64229.

[66]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., &Sethii, S. (2019). Designing the Integration Layer. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 149-179.

DOI https://doi.org/10.1007/978-1-4842-4303-9_5

[67]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., &Sethii, S. (2019). DXP Performance Optimization. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 235-259.

DOI https://doi.org/10.1007/978-1-4842-4303-9_9

[68]. Shivakumar, S. K., &Sethii, S. (2019). Building Digital Experience Platforms.

https://link.springer.com/book/10.1007/978-1-4842-4303-9

[69]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., &Sethii, S. (2019). Quality Attributes and Sizing of the DXP. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 215-234.

DOI https://doi.org/10.1007/978-1-4842-4303-9_8

[70]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., &Sethii, S. (2019). End to End DXP Case Study. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 299-320.

DOI https://doi.org/10.1007/978-1-4842-4303-9_11

[71]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., &Sethii, S. (2019). Transforming legacy banking applications to banking experience platforms. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 261-295.

DOI https://doi.org/10.1007/978-1-4842-4303-9_10

[72]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., &Sethii, S. (2019). DXP Information Security. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 201-212.

DOI https://doi.org/10.1007/978-1-4842-4303-9_7

[73]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., &Sethii, S. (2019). Introduction to Digital Experience Platforms. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 3-26.

DOI https://doi.org/10.1007/978-1-4842-4303-9_1

[74]. Sethi, S. (2023). Platforms Based Approach and Strategy for Fintech applications. *Authorea Preprints*.

DOI https://doi.org/10.36227/techrxiv.24329533.v1

[75].Latif, M. A., Mushtaq, Z., Arif, S., Rehman, S., Qureshi, M. F., Samee, N. A., ... & Al-masni, M. A. Improving Thyroid Disorder Diagnosis via Ensemble Stacking and Bidirectional Feature Selection.

DOI https://doi.org/10.32604/cmc.2024.047621

[76]. Tomar, M., &Periyasamy, V. (2023). The Role of Reference Data in Financial Data Analysis: Challenges and Opportunities. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 1(1), 90-99.

DOI: https://doi.org/10.60087/jklst.vol1.n1.p99

[77]. Chentha, A. K., Sreeja, T. M., Hanno, R., Purushotham, S. M. A., &Gandrapu, B. B. (2013). A Review of the Association between Obesity and Depression. Int J Biol Med Res, 4(3), 3520-3522.

[78]. Gadde, S. S., &Kalli, V. D. R. (2020). Descriptive analysis of machine learning and its application in healthcare. *Int J Comp Sci Trends Technol*, *8*(2), 189-196.

[79]. Atacho, C. N. P. (2023). A Community-Based Approach to Flood Vulnerability Assessment: The Case of El Cardón Sector. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 434-482. DOI:https://doi.org/10.60087/jklst.vol2.n2.p482

[80]. jimmy, fnu. (2023). Understanding Ransomware Attacks: Trends and Prevention Strategies. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(1), 180-210. https://doi.org/10.60087/jklst.vol2.n1.p214

[81]. Bayani, S. V., Prakash, S., &Malaiyappan, J. N. A. (2023). Unifying Assurance A Framework for Ensuring Cloud Compliance in AIML Deployment. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3), 457-472.DOI: https://doi.org/10.60087/jklst.vol2.n3.p472

[82]. Bayani, S. V., Prakash, S., &Shanmugam, L. (2023). Data Guardianship: Safeguarding Compliance in AI/ML Cloud Ecosystems. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3), 436-456.

DOI: https://doi.org/10.60087/jklst.vol2.n3.p456

[83]. Karamthulla, M. J., Malaiyappan, J. N. A., & Prakash, S. (2023). AI-powered Self-healing Systems for Fault Tolerant Platform Engineering: Case Studies and Challenges. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 327-338. DOI: https://doi.org/10.60087/jklst.vol2.n2.p338

[84]. Prakash, S., Venkatasubbu, S., &Konidena, B. K. (2023). Unlocking Insights: AI/ML Applications in Regulatory Reporting for US Banks. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *1*(1), 177-184.DOI: https://doi.org/10.60087/jklst.vol1.n1.p184

[85]. Prakash, S., Venkatasubbu, S., &Konidena, B. K. (2023). From Burden to Advantage: Leveraging AI/ML for Regulatory Reporting in US Banking. *Journal of Knowledge Learning*

and Science Technology ISSN: 2959-6386 (online), *1*(1), 167-176. DOI: https://doi.org/10.60087/jklst.vol1.n1.p176

[86]. Prakash, S., Venkatasubbu, S., &Konidena, B. K. (2022). Streamlining Regulatory Reporting in US Banking: A Deep Dive into AI/ML Solutions. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *1*(1), 148-166.DOI: https://doi.org/10.60087/jklst.vol1.n1.p166

[87]. Tomar, M., &Jeyaraman, J. (2023). Reference Data Management: A Cornerstone of Financial Data Integrity. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(1), 137-144.DOI: https://doi.org/10.60087/jklst.vol2.n1.p144

[88]. Tomar, M., &Periyasamy, V. (2023). The Role of Reference Data in Financial Data Analysis: Challenges and Opportunities. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 1(1), 90-99.

DOI: https://doi.org/10.60087/jklst.vol1.n1.p99

[89]. Tomar, M., &Periyasamy, V. (2023). Leveraging Advanced Analytics for Reference Data Analysis in Finance. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(1), 128-136.

DOI: https://doi.org/10.60087/jklst.vol2.n1.p136

[90]. Sharma, K. K., Tomar, M., &Tadimarri, A. (2023). Unlocking Sales Potential: How AI Revolutionizes Marketing Strategies. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 231-250.

DOI: https://doi.org/10.60087/jklst.vol2.n2.p250

[91]. Sharma, K. K., Tomar, M., &Tadimarri, A. (2023). Optimizing Sales Funnel Efficiency: Deep Learning Techniques for Lead Scoring. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 261-274.

DOI: https://doi.org/10.60087/jklst.vol2.n2.p274

[92]. Shanmugam, L., Tillu, R., &Tomar, M. (2023). Federated Learning Architecture: Design, Implementation, and Challenges in Distributed AI Systems. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 371-384.

DOI: https://doi.org/10.60087/jklst.vol2.n2.p384

[93]. Sharma, K. K., Tomar, M., &Tadimarri, A. (2023). AI-driven Marketing: Transforming Sales Processes for Success in the Digital Age. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 250-260.

DOI: https://doi.org/10.60087/jklst.vol2.n2.p260

[94]. Gadde, S. S., &Kalli, V. D. (2021). The Resemblance of Library and Information Science with Medical Science. International Journal for Research in Applied Science & Engineering Technology, 11(9), 323-327.

[95]. Gadde, S. S., &Kalli, V. D. R. (2020). Technology Engineering for Medical Devices-A Lean Manufacturing Plant Viewpoint. Technology, 9(4).

[96]. Gadde, S. S., &Kalli, V. D. R. (2020). Medical Device Qualification Use. International Journal of Advanced Research in Computer and Communication Engineering, 9(4), 50-55.

[97]. Gadde, S. S., &Kalli, V. D. R. (2020). Artificial Intelligence To Detect Heart Rate Variability. *International Journal of Engineering Trends and Applications*, *7*(3), 6-10.

[98]. Chentha, A. K., Sreeja, T. M., Hanno, R., Purushotham, S. M. A., &Gandrapu, B. B. (2013). A Review of the Association between Obesity and Depression. *Int J Biol Med Res*, *4*(3), 3520-3522.

[99]. Tao, Y. (2022). Algorithm-architecture co-design for domain-specific accelerators in communication and artificial intelligence (Doctoral dissertation).

https://deepblue.lib.umich.edu/handle/2027.42/172593

[100]. Tao, Y., Cho, S. G., & Zhang, Z. (2020). A configurable successive-cancellation list polar decoder using split-tree architecture. IEEE Journal of Solid-State Circuits, 56(2), 612-623.

DOI: https://doi.org/10.1109/JSSC.2020.3005763

[101]. Tao, Y., & Choi, C. (2022, May). High-Throughput Split-Tree Architecture for Nonbinary SCL Polar Decoder. In 2022 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 2057-2061). IEEE.

DOI: https://doi.org/10.1109/ISCAS48785.2022.9937445

[102]. Tao, Y. (2022). Algorithm-architecture co-design for domain-specific accelerators in communication and artificial intelligence (Doctoral dissertation).

https://deepblue.lib.umich.edu/handle/2027.42/172593

[103]. Mahalingam, H., VelupillaiMeikandan, P., Thenmozhi, K., Moria, K. M., Lakshmi, C., Chidambaram, N., &Amirtharajan, R. (2023). Neural attractor-based adaptive key generator with DNA-coded security and privacy framework for multimedia data in cloud environments. Mathematics, 11(8), 1769.

https://doi.org/10.3390/math11081769

[104]. Padmapriya, V. M., Thenmozhi, K., Praveenkumar, P., &Amirtharajan, R. (2020). ECC joins first time with SC-FDMA for Mission "security". Multimedia Tools and Applications, 79(25), 17945-17967.

DOI https://doi.org/10.1007/s11042-020-08610-5

[105]. Padmapriya, V. M. (2018). Image transmission in 4g lte using dwt based sc-fdma system. Biomedical & Pharmacology Journal, 11(3), 1633.

DOI :https://dx.doi.org/10.13005/bpj/1531

[106]. Padmapriya, V. M., Priyanka, M., Shruthy, K. S., Shanmukh, S., Thenmozhi, K., &Amirtharajan, R. (2019, March). Chaos aided audio secure communication over SC-FDMA system. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) (pp. 1-5). IEEE.

https://doi.org/10.1109/ViTECoN.2019.8899413

[107]. Padmapriya, V. M., Thenmozhi, K., Praveenkumar, P., &Amirtharajan, R. (2022). Misconstrued voice on SC-FDMA for secured comprehension-a cooperative influence of DWT and ECC. Multimedia Tools and Applications, 81(5), 7201-7217.

DOI https://doi.org/10.1007/s11042-022-11996-z

[108]. Padmapriya, V. M., Sowmya, B., Sumanjali, M., &Jayapalan, A. (2019, March). Chaotic Encryption based secure Transmission. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) (pp. 1-5). IEEE.

DOI https://doi.org/10.1109/ViTECoN.2019.8899588

[109]. Sowmya, B., Padmapriya, V. M., Sivaraman, R., Rengarajan, A., Rajagopalan, S., &Upadhyay, H. N. (2021). Design and Implementation of Chao-Cryptic Architecture on FPGA for Secure Audio Communication. In Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, Volume 3 (pp. 135-144). Springer Singapore

https://link.springer.com/chapter/10.1007/978-981-15-9774-9_13

[110]. Padmapriya, V. M., Thenmozhi, K., Avila, J., Amirtharajan, R., &Praveenkumar, P. (2020). Real Time Authenticated Spectrum Access and Encrypted Image Transmission via Cloud Enabled Fusion centre. Wireless Personal Communications, 115, 2127-2148.

DOI https://doi.org/10.1007/s11277-020-07674-8

[111].Thakur, A., & Thakur, G. K. (2024). Developing GANs for Synthetic Medical Imaging Data: Enhancing Training and Research. Int. J. Adv. Multidiscip. Res, 11(1), 70-82.

DOI: http://dx.doi.org/10.22192/ijamr.2024.11.01.009

[112]. Shuford, J. (2023). Contribution of Artificial Intelligence in Improving Accessibility for Individuals with Disabilities. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(2), 421-433.DOI: https://doi.org/10.60087/jklst.vol2.n2.p433

[113]. Schwartz, E. A., Bravo, J. P., Ahsan, M., Macias, L. A., McCafferty, C. L., Dangerfield, T. L., ...& Taylor, D. W. (2024). RNA targeting and cleavage by the type III-Dv CRISPR effector complex. Nature Communications, 15(1), 3324.

https://www.nature.com/articles/s41467-024-47506-y#Abs1

[114]. Saha, A., Ahsan, M., Arantes, P. R., Schmitz, M., Chanez, C., Jinek, M., & Palermo, G. (2024). An alpha-helical lid guides the target DNA toward catalysis in CRISPR-Cas12a. Nature Communications, 15(1), 1473.https://www.nature.com/articles/s41467-024-45762-6

[115]. Nierzwicki, Ł., Ahsan, M., & Palermo, G. (2023). The electronic structure of genome editors from the first principles. Electronic Structure, 5(1), 014003.DOI https://doi.org/10.1088/2516-1075/acb410

[116]. Bali, S. D., Ahsan, M., &Revanasiddappa, P. D. (2023). Structural Insights into the Antiparallel G-Quadruplex in the Presence of K+ and Mg2+ Ions. The Journal of Physical Chemistry B, 127(7), 1499-1512.https://doi.org/10.1021/acs.jpcb.2c05128

[117]. Ahsan, M., Pindi, C., &Senapati, S. (2022). Mechanism of darunavir binding to monomeric HIV-1 protease: A step forward in the rational design of dimerization inhibitors. Physical Chemistry Chemical Physics, 24(11), 7107-7120.https://doi.org/10.1039/D2CP00024E

[118]. Ahsan, M., Pindi, C., &Senapati, S. (2021). Hydrogen bonding catalysis by water in epoxide ring opening reaction. Journal of Molecular Graphics and Modelling, 105, 107894.https://doi.org/10.1016/j.jmgm.2021.107894

[119]. Ahsan, M., Pindi, C., &Senapati, S. (2020). Electrostatics plays a crucial role in HIV-1 protease substrate binding, drugs fail to take advantage. Biochemistry, 59(36), 3316-3331.

https://doi.org/10.1021/acs.biochem.0c00341

[120]. Pindi, C., Chirasani, V. R., Rahman, M. H., Ahsan, M., Revanasiddappa, P. D., &Senapati, S. (2020). Molecular basis of differential stability and temperature sensitivity of ZIKA versus dengue virus protein shells. Scientific Reports, 10(1), 8411.https://doi.org/10.1038/s41598-020-65288-3

[121]. Ahsan, M., &Senapati, S. (2019). Water plays a cocatalytic role in epoxide ring opening reaction in aspartate proteases: a QM/MM study. *The Journal of Physical Chemistry B*, *123*(38), 7955-7964.

https://doi.org/10.1021/acs.jpcb.9b04575

[122]. Dixit, S. M., Ahsan, M., &Senapati, S. (2019). Steering the lipid transfer to unravel the mechanism of cholesteryl ester transfer protein inhibition. Biochemistry, 58(36), 3789-3801.

https://doi.org/10.1021/acs.biochem.9b00301

[123]. Hasan, M. R., Gazi, M. S., & Gurung, N. (2024). Explainable AI in Credit Card Fraud Detection: Interpretable Models and Transparent Decision-making for Enhanced Trust and Compliance in the USA. *Journal of Computer Science and Technology Studies*, *6*(2), 01-12.

[124]. Gazi, M. S., Hasan, M. R., Gurung, N., & Mitra, A. (2024). Ethical Considerations in AI-driven Dynamic Pricing in the USA: Balancing Profit Maximization with Consumer Fairness and Transparency. *Journal of Economics, Finance and Accounting Studies*, *6*(2), 100-111.

[125]. Sarkar, M., Puja, A. R., & Chowdhury, F. R. (2024). Optimizing Marketing Strategies with RFM Method and K-Means Clustering-Based AI Customer Segmentation Analysis. *Journal of Business and Management Studies*, *6*(2), 54-60.

[126]. Jones, K., Spaeth, J., Rykowski, A., Manjunath, N., Vudutala, S. K., Malladi, R., & Mishra, A. (2020). U.S. Patent No. 10,659,295. Washington, DC: U.S. Patent and Trademark Office.

[127]. Malladi, R., Bukkapattanam, A., Wigley, C., Aggarwal, N., & Vudutala, S. K. (2021). U.S. Patent No. 11,087,020. Washington, DC: U.S. Patent and Trademark Office.

[128]. Jones, K., Pitchaimani, S., Viswanathan, S., Shah, M., Malladi, R., Allidina, A., ... & Brannon, J. B. (2023). U.S. Patent No. 11,797,528. Washington, DC: U.S. Patent and Trademark Office.