Paradigm Academic Press
Art and Society
ISSN 2709-9830
OCT. 2025 VOL.4, NO.9

# Vulnerability of Cyber Security Is an Unexpected Threat to Global Internet System

Haradhan Kumar Mohajan[1]

[1] Chairman and Associate Professor, Department of Mathematics, Premier University, Chittagong, Bangladesh

Correspondence: Haradhan Kumar Mohajan, Chairman and Associate Professor, Department of Mathematics, Premier University, Chittagong, Bangladesh.

doi:10.63593/AS.2709-9830.2025.10.001

**Abstract**

At present the world is becoming highly interconnected, and cyber security is essential for the sustainability and development of the global networking. Cyber security is the practice of protecting digital devices, networks, and sensitive data from cyber threats, such as hacking, malware, and phishing attacks that are committed over the internet by technically skilled criminals, who have a wide range of strategies, technologies, and best practices. It is an urgent national and global problem. At present it becomes an incredibly complex and changing policy and important issue in the infrastructure of every company and organization. Data in computer can be lost or destroyed through physical and natural disasters, such as floods, fires, and unexpected catastrophes done by the cyber criminals. The purpose of this study is to discuss the aspects of cyber security for the improvement of the safety and security of cyber space.

**Keywords:** cybercrime, cyber security, information security, network

## 1. Introduction

At present the world is becoming increasingly digital, and more than 5.4 billion people worldwide use internet for the personal, economical, commercial, cultural, social, and governmental activities (Li & Liu, 2021). Our life is fully dependent on cell phone, computer, information technology (IT) infrastructures, power grids, air traffic management systems, industrial manufacturing, and banking sectors (Iqbal et al., 2020). The growth in e-commerce, digital payments, digital transformation initiatives, internet and mobile usage, and cloud computing adoption has modernized the world (Lehto & Neittaanmäki, 2015). In 2023, global retail e-commerce sales are estimated at $5.8 trillion, and it is estimated that by 2027 it will reach to $8 trillion (Mouna & Yassine, 2024). In 2025, the digital transformation market may reach to $1,009.8 billion, and it is estimated that it will reach to $3.9 trillion by 2027 (Danturthi, 2024).

Cyber security is the wide range of protection of computer system meant little-to-no security and the data security on various types of networks that they are stored and accessed by users. It consists of practices, analysis, and technologies that assist to keep computer systems and digital data secure. It is the combination of methods, processes, tools, and behaviors that protect computer systems, networks, and data from cyber-attacks and unauthorized access (Belapure & Godbole, 2011). It remains one of the serious and widespread challenges for financial institutions around the world. It is the field of technologies, processes, and activities designed to protect the individuals from hackers, viruses, and malwares. It is the idea of engineering that continues to function correctly against a malicious attack. Sometimes it depends on people related to its operation, such as human error, negligence, and lack of awareness (Kumar et al., 2018).

Elements of cyber security are network security, application security, endpoint security, data security, identity management, database and infrastructure security, cloud security, mobile security, disaster recovery, etc. There

are three levels of security as, basic, enhanced, and critical (Cabaj et al., 2018). According to Forbes, the global cyber security market reached to $75 billion for 2015 and about $170 billion in 2020. Some of the dangerous cybercrimes are cyber-stalking, cyber-terrorism, email spoofing, email bombing, cyber pornography, cyber-defamation, etc. (Goni, 2022; Mohajan, 2025a). Various tools that can be used for preventing the hacking are Honeynet, anti-viruses, patches, password crackers, vulnerability scanners, and wireless sniffers. By following best practices, staying informed, and adhering to security protocols, individuals can play a crucial role in preventing breaches and can keep networking systems safe (Moore, 2005).

## 2. Literature Review

A literature review is an overview of previously published works on a particular topic that is a comprehensive summary, analysis, and synthesis of existing scholarly works on a specific topic (Bolderston, 2008). It is a vital part of a research project, paper, and thesis that shows how to organize and synthesize information, and demonstrates the ability to write any kind of research article (Torraco, 2016). A good literature review has a proper research question, a proper theoretical framework, and a chosen research methodology (Baker, 2000). The main types of narrative reviews are evaluative, exploratory, and instrumental (Creswell, 2013a). Mohammad Nur Nabi and Muhammad Tanjimul Islam have realized that with the rapid spread of information and communication technology (ICT) worldwide, cybercrime appears to be a potential threat for confidential computer data and systems, and Bangladesh is under risk of cybercrimes that threatens the national security of the country due to lack of advanced cyber technologies and lack of awareness (Nabi & Islam, 2023). Deepansh Kumar and his coworkers have shown that the rising growth of the internet and computer technology has brought many good and proficient things for people, such as e-commerce, email, cloud computing, and data sharing. But it also has dark and hidden sides, such as network hacks, computer hacks, mobile breach, backdoors, etc. The cybercrime is one of the common practices made by the computer experts and is increasing rapidly in numbers that is responsible for disrupting the organization networks, stealing valuable data, documents, and hacking bank account. They have discussed the types of hackers, and the categories of different IT networks with their weaknesses (Kumar et al., 2018).

Rohit Kalakuntla and his coauthors have shown that cyber security is a significant worry to all nations. They have emphasized on cyber security and cyber terrorism (Kalakuntla et al., 2019). Aleksandra Kuzior and her coworkers have tried to analyze the global trends in cybercrime to form a global, open and safe cyberspace, protect the population from cyber threats and cyber fraud, increase the effectiveness of financial monitoring procedures, and control over transactions in cyberspace (Kuzior et al., 2024). Ibrahim Sisaneci and his coworkers have shown that broader use of digital technologies in all aspects of our lives, exponential expansion of cyberspace, along with complex and advanced cyber threats, cyber security becomes important and essential (Sisaneci et al., 2013). Mohan V. Pawar and J. Anuradha have described the network security confidentiality vector, network security integrity vector, and network security availability vector. They have realized that protection of computer and network security are critical issues, because many types of attacks are increasing day by day (Pawar & Anuradha, 2015).

Buket Erşahin and Mustafa Erşahin have shown how security flaws of web applications can threat information security, and also have focused on how web developers can already prevent security problems during the development life cycle (Erşahin & Erşahin, 2022). Hamed Taherdoost has provided various definitions of cyber security and information security with their differences. Both are related to the security of data aiming to defend data against different types of cyber threats, but they should not be used interchangeably. Information security means protecting information system from unauthorized access, use, disclosure, disruption, modification, and destruction. On the other hand, cyber security is the wide range of protection of computer system meant little-to-no security (Taherdoost, 2022). P. K. Paul and P. S. Aithal have stated that cloud security is the set of policies, technologies, applications, and control utilized for virtual infrastructure that includes hardware, software, and application. It is very close to computer security, IT security, and information security. They have described different areas of cloud security (Paul & Aithal, 2019). Mohamed Litoussi and his coauthors have shown that Internet of Things (IoT) dramatically influences our daily lives in several domains, ranging from teeny wearable devices to large industrial systems. Although IoT enhance quality of human life, it is vulnerable to various cyber-attacks, and needs challenging techniques to achieve their security (Litoussi et al., 2020). Mychael Maoeretz Engel and his coauthors have contributed to the academic and practical side of mobile device, and can guide future research for system development related to its security (Engel et al., 2022).

## 3. Research Methodology of the Study

Research is the search for knowledge that is closely related to the object of study. It is a systematic inquiry to describe, explain, predict, and control the observed phenomenon (Babbie, 2009). It is the creation of new knowledge and the use of existing knowledge in a new and creative way for generating new concepts, methodologies, and understandings that involves inductive and deductive methods (Groh, 2018). There are two

major types of empirical research design: qualitative research and quantitative research (Mohajan, 2017). Researchers choose any one of these according to the nature of the research topic they want to investigate. Qualitative research involves collecting non-numerical data and identifying patterns in language, theme, and structure, among other features to understand human experiences. Instruments for qualitative research include questionnaires, interviews, and observations (Creswell, 2013b; Mohajan, 2018b). Quantitative research involves collecting numerical data and conducting mathematical analyses to observe trends, make predictions, run experiments, and test hypotheses (Mohajan, 2020; Ghanad, 2023).

A methodology is a branch of knowledge that deals with the methods of a particular discipline (Mohajan, 2018a). It is the system of methods followed consistently that refers either to a method, the field of inquiry studying methods, and philosophical discussions of background assumptions involved (Bryman, 2008). It describes how the research is conducted. The goal of methodology is to increase the credibility of the research by making process transparent and reproducible of the researcher (Howell, 2013). Research methodology is a systematic approach that details how a researcher will conduct the study to find a reliable and valid answer to a research question. It describes and explains the techniques and procedures used to identify and analyze information regarding a specific research topic (Shields & Rangarjan, 2013). In this study, I have discussed the cybercrime in briefly. I have stressed on the types of cyber security in some details. There are many types of cyber security in the cyber space. I have discussed twelve types of cyber security i) network security, ii) application security, iii) information security, iv) internet of things (IoT) security, v) cloud security, vi) operational security, vii) mobile security, viii) operational technology (OT) security, ix) GenAI security, x) secure access service edge (SASE), xi) zero trust security, and xii) endpoint security (Pawar & Anuradha, 2015).

## 4. Objective of the Study

In 2015, cybercrime cost the world $500 billion, $3 trillion, and $6 trillion in 2015, 2018, and 2021 respectively. Cyber security indicates that computers and network systems are protected from threats and vulnerabilities, and these systems work efficiently (Zhang et al., 2021). Passwords are important aspects of computer security, and a poorly chosen password may result in unauthorized access (Taherdoost, 2022). Network security, database security, online security, cloud security, etc. are all closely connected to cyber security. Without an effective cyber security strategy organizations become easy targets for cybercriminals (Nabi & Islam, 2023). Main objective of this study is to discuss the aspects of global cyber security. Other minor objectives of the study are as follows:

1) to highlight on cybercrime, and
2) to discuss the types of cyber security.

## 5. Cybercrime

There is no universally accepted definition of cybercrime. It is a widespread and lucrative illicit activity and a major threat to the society that uses a computer as its main means of commissioning or theft, which involves code-imposed offences, such as network intrusions and computer virus distributors, and web-based forms of traditional crimes, such as identity theft, harassment, intimidation and extremism that have become a major problem for individuals and nations (Iqbal et al., 2020).

At present cybercrime is a crucial topic due to the widespread and evolving nature of cyber threats, the growing dependency on digital systems, and the significant impacts on economic, personal, and national security (Kuzior et al., 2024). It is a criminal activity that occurs at all levels of society and takes many forms, from investment fraud to phishing and the creation of bogus entities (Mohajan, 2025d). It has numerous targets, such as email fraud, spamming, hacking, malware, online gambling, child exploitation, phishing, ransomware, social media crime, denial of service, ATM fraud, fraud credit card, misinformation, social engineering, identity theft, Trojan, data theft, cyber-stalking, cyber bulling, cyber harassment, fake call, online transactions fraud, insurance fraud, cyber terrorism, etc. (Sang & Trung, 2022).

It can be characterized into two different categories: cyber-dependent crimes, and cyber-enabled crimes. Cyber-dependent crime is any crime that can only be committed using computers, computer networks or other forms of information communication technology that targets ICT systems and are typified by hacking, ransomware, and malware (Murphy, 2024). Cyber-enabled crime is traditional crimes facilitated by the internet and digital technologies that has evolved in scale and form through the increased use of the internet and communication technology, such as fraud through phishing, piracy, and counterfeiting (Shahidullah et al., 2022).

## 6. Types of Cyber Security

Cyber security is a convergence of multiple approaches that cover several strategies and practices. It encompasses specialized areas protecting digital systems, networks, and data. It remains one of the top concerns facing individuals, businesses, and governments (Schmidt, 2014). In this section, I have discussed twelve

essential types of cyber security i) network security, ii) application security, iii) information security, iv) internet of things (IoT) security, v) cloud security, vi) operational security, vii) mobile security, viii) operational technology (OT) security, ix) GenAI security, x) secure access service edge (SASE), xi) zero trust security, and xii) endpoint security (Feruza & Kim, 2007).

*6.1 Network Security*

The world is becoming more interconnected of the internet with new networking technology. Modern internet technology protects confidential data, employee information, business models, and identity and resources. Actually, there exists a "communication gap" between the developers of security technology and developers of networks (Pawar & Anuradha, 2015). Network security is the policies, technologies, practices, controls, and procedures used of protecting the integrity, confidentiality, and accessibility of computer networks and data from unauthorized access, misuse, modification, data breaches, network-accessible resources, denial of a computer network, and other network-based threats (Krawczyk-Sokołowska & Caputa, 2023). It safeguards communication infrastructure, such as devices, hardware, software, and communication protocols. It covers a variety of computer networks, both public and private that are used in everyday jobs for conducting transactions and communications among businesses, military, government agencies, and individuals (Macfarlane et al., 2012). It protects data integrity, confidentiality, and availability as information travels over a network and between network-accessible assets. It is a main issue of computing because many types of attacks are increasing day by day. It is a challenge for network operators and internet service providers to prevent it from the attack of intruders (Ghansela, 2013).

Network security should detect, monitor, and block attacks that seek unauthorized access to the network that is done by using VPNs, intrusion detection and prevention systems, and firewalls. It starts with authentication, commonly with a username and a password that uses a combination of letters, numbers, special characters, and a space, and it is sometimes termed one-factor authentication. Sometimes two-factor authentication, such as security token, ATM card, and a mobile phone are used. Also, three-factor authentication, such as fingerprint and retinal scan are also used (Pawar & Anuradha, 2015). Networking faces three categories of attacks: active attack, passive attack, and advance attack. Active attack happens when an intruder initiates commands to disrupt the normal network operation. Some active attacks are spoofing attack, wormhole attack, modification, denial of services, fabrication, sinkhole, and sybil attack (Dowd & McHenry, 1998). Passive attack happens when a network intruder intercepts data traveling through the network. Some passive attacks are traffic analysis, eavesdropping, and monitoring. Advance attacks are black hole attack, replay attack, byzantine attack, and location disclosure attack (Chahar, 2022). Anti-virus software, intrusion prevention system helps to detect and inhibit the action of malware. Honeypots are placed at a point in the network where they appear vulnerable and undefended (Patnaik, 2021).

*6.2 Application Security*

Application software is one of the important components that fuel the so-called third-platform, which is congregation of social, mobile, analytics with big data, and cloud computing technology (Rajendran, 2015). Google Play has 3,553 million, Apple App Store has 1,642 million, and Amazon App Store has 483 million applications (Danturthi, 2024). As Apps become more ubiquitous, interconnected, and complex; finding and fixing the growing volume of vulnerabilities just gets more challenging. There are mainly two types of applications: mobile applications and web based applications (Chandrasekaran, 2024). Mobile devices are being used to access a range of services from social networking, banking, ticketing, and shopping to corporate applications, such as email, enterprise resource planning, customer relationship management, and calendar and address book applications (Shin & Williams, 2008). A web App is application software that is created with web technologies and runs via a web browser. It is a branch of information security that deals specifically with the security of websites, web applications, and web services. It is emerged in the late 1990s and allowed for the server to dynamically build a response to the request, in contrast to static web pages (Hoffman, 2020). Evolution of the World Wide Web (www) has created web applications with greater abilities, and fast growing and evolving web environment brings up its own risks (Erşahin & Erşahin, 2022).

Secure controls, such as strong authentication, granular permission, and data encryption can help to lower the risk of data leaks and unauthorized access. Application security (AppSec) is all tasks that introduce a secure software development of the whole life cycle from requirements analysis, design, implementation, verification as well as maintenance to development teams (Shuaibu et al., 2013). It involves secure coding practices, processes, tools, regular software updates and patches, and application-level firewalls that help prevent data breaches and protect applications. It refers to the technologies, policies, procedures, process of identifying and repairing vulnerabilities in application software to prevent unauthorized access, modification, or misuse. Use of secure coding rules and practices is necessary to create strong and reliable applications (Li & Xue, 2011).

The AppSec is necessary to effectively eliminate, reduce, and mitigate the overall risks from the application

attack surface, for the overall development, security, and operations process. It involves a combination of mitigation strategies during application development and after deployment. A strong AppSec program improves the security posture of organizations and helps them proactively find, fix, and prevent security issues in their applications (McDonald, 2020). About 62% of cyber security professionals are at best moderately confident in their organization's application security posture. Most of the Apps that we use on our cell phones are secured and work under the rules and regulations of the Google Play Store (Das & Johnson, 2021).

*6.3 Information Security*

We use the internet looking for information, doing social networking, banking, shopping, and lots of other online functions (Mohajan, 2025b). Nowadays living without access to the information of interest at any time and any place through countless types of devices has become unimaginable (Alhassana & Adjei-Quayeb, 2017). Information technology is the vehicle that stores and transports information that is a most valuable resource of a company (Reid & van Niekerk, 2014). It may be electronic soft copy, hard copy, delivered in conversation and films, and any other sensitive data, such as documents, personal photos, emails, conversations, and important numbers (Santos, 2020). Confidentiality of information ensures that only those with sufficient privileges may access certain information. When unauthorized individuals can access information, confidentiality is broken (Susanto & Almunawar, 2022).

Often cyber security and information security are used interchangeably, but there are differences in each concept. Information security is concentrated to protect information everywhere, whereas cyber security is specifically focused on information in cyberspace (Taherdoost, 2022). Information security (InfoSec) is the security of computer systems to protect them against disclosure, subjective modification, unauthorized access, harassment, and destruction that aim to ensure integrity, confidentiality, and availability of information (Wendy & Wang, 2019). It refers to the tools and processes for preventing, detecting, and remediating threats to sensitive information, whether digitized or not. It is an attempt to create a framework for ensuring confidentiality, integrity, and availability of information (Andress, 2014). Also, the preservation of authenticity, privacy, accountability, non-repudiation, auditability, and reliability are essential for information security (Layton, 2007). Information security indicates the protection of information against different threats that aim to minimize the risk of business activities, maximize return on investments, exploit business opportunities, and ensuring continuity of business (Dhillon, 2007). Various supportive tools are used to InfoSec, such as anti-virus, anti-spyware, software, windows and applications updates, firewalls, content filtering, parental control, smart encryption codes and techniques, methods, and advices related to security (Feruza & Kim, 2007).

Information security is the practice of protecting sensitive information from unauthorized access, disclosure, modification, alteration, disruption, and destruction of information security management, computer and data security, and network security. It includes encryption, access controls, data classification, and data loss prevention (DLP) measures (Joshi et al., 2017). It also prevents or reduces the probability of unauthorized access to data for the unlawful use, theft or vandalism, disclosure, power failures, disruption, deletion, corruption, modification, natural disasters, adverse environmental conditions, inspection, recording, and devaluation of information (Daniel & Titman, 2006).

*6.4 Cloud Security*

Cloud computing is one of the most popular information technologies that is used to reduce its operating costs, increase revenue, and develop fast-growing IT industry; and the key point in them is cloud computing security (Malallah et al., 2023). It is considered as a modern generation in the information technology revolution that provides a wide range for sharing services through the internet, such as data storage, servers, databases, networking, and software (L'Esteve, 2023). It has three components: clients, distributed servers, and data centers. It has revolutionized the way of storing, processing, and managing data; offering unprecedented levels of flexibility, scalability, and efficiency (Ang'udi, 2023). The cloud computing can be implemented in four deployment models as (Rittinghouse & Ransome, 2009): i) a public cloud is made available to the general public or large industry group and is owned, managed, and operated by a business, academic, or government, where third-party providers deliver computing resources, such as servers, storage, networking, and applications (Velev & Zlateva, 2011), ii) a private cloud is operated entirely for a single customer or organization that may be managed by a third-party provider that offers superior control, security, and customization compared to public clouds (Gupta et al., 2019), iii) a community cloud is owned, managed, operated, and shared by several organizations; and supports of a specific community that have common goals, security requirements, or regulatory needs and may be managed by the organizations or a third party (Mondal et al., 2020), iv) a hybrid cloud combines and unifies public cloud, private cloud and on-premises infrastructure to create a single, flexible, cost-optimal IT infrastructure (Reese, 2009).

Cloud computing faces serious security risks, such as data loss, privacy violations, financial damages, distributed denial of service, and erosion of user trust that require careful attention (Singh & Chatterjee, 2017). Moreover,

dynamic and scalable nature of cloud services complicates the task of ensuring consistent security across different service models and deployment models (Seifert et al., 2023). Cloud security is a multifaceted discipline that refers to the technologies, policies, controls, procedures, applications, and services that protect the vast array of data, applications, and infrastructure of cloud environments. It is very close with the network security, database security, web security, etc. (Malik et al., 2023). It uses various cloud service providers, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), Amazon Web Services (AWS), Azure, Google Cloud, etc., to ensure security against multiple threats (Srinivasan et al., 2012). It enhances privacy if configured and managed correctly and saves data on the cloud, making it accessible from any device with proper authentication (Butt et al., 2023). It is crucial for the safe, secure storage of data and other items in cloud systems. It is applicable in different types of organizations and institutions including government organizations and bodies. It has become a popular option over the last decade (Paul & Aithal, 2019).

*6.5 Internet of Things (IoT) Security*

The Internet of Things (IoT) is a vast network of interconnected devices, objects, and services that collect and exchange data to improve efficiencies and create new opportunities in various industries. These aspire to connect anyone with anything at any point of time at any place, and provide the connectivity between objects timelessly (Najar, 2019). These devices have attracted considerable attention during the past few years. These range from everyday household appliances, such as smart thermostats and lighting systems to large-scale industrial machineries, such as manufacturing equipment and transportation vehicles (Tawalbeh et al., 2020). These create a new era in which all technologies and appliances are connected to the internet, and users can use them together to complete complex operations easily. The IoT world has a huge variety of devices, such as smartphones, personal computers, PDAs, laptops, tablets, and other hand-held embedded devices (Said & Zolkipli, 2022). The term “Internet of Things” was originally coined by Kevin Ashton, British technology pioneer and a co-founder of the Auto-ID Center at the Massachusetts Institute of Technology (MIT) Auto-ID Centre in 1999 (Kramp et al., 2013). At present the number IoT devices worldwide are 19.8 billion in 2025, and it is expected to be more than 40.6 billion by 2034 (Kalsi et al., 2023).

The IoT security is the technology segment focused on safeguarding connected devices and networks in the IoTs, such as smart home gadgets, industrial sensors, medical equipment, and wearable technology from cyber threats (Rao & Haq, 2018). It focuses on protecting, monitoring and remediating threats related to these devices, and ensures that these devices do not become entry points for hackers to exploit networks and steal sensitive data. It refers to a network within which information from all connected devices can be gathered, processed, and modified to offer new services (Litoussi et al., 2020).

The IoT promises technical advances, improves efficiencies, provides greater revenues, and enhances customer experiences. This clearly indicates that IoT is becoming mainstream and representing a significant opportunity for the global economy, society and business. However, this expansion heightens security as a major concern (Miorandi et al., 2012). It also faces various security and privacy issues and challenges, and the majority of the security threats are related to leakage of information and loss of services that are related to confidentiality, integrity, authentication, etc. Hence, a secure mechanism is needed to protect the personal information (Ziegeldorf et al., 2014). It is of three-layer architecture, and its security principles should be enabled at each layer for the proper and efficient working of the applications. The era of IoT has enhanced the life quality our living styles by connecting various smart devices, technologies, and applications. The IoT is applied in healthcare, transportation, lifestyle, smart home, smart city, retail, supply chain, agriculture, smart factory, emergency, user interaction, culture and tourism, environment and energy (Geneiatakis et al., 2017).

*6.6 Operational Security*

Operational security (OPSEC) is a strategic process and policy that is used to protect sensitive information from falling into the wrong hands by identifying critical data, assessing threats and vulnerabilities, and implementing countermeasures with internal threats and human errors (Vick, 2015). It refers to the choices, technologies, and activities through which information assets as well as sensitive systems are protected and handled (Mohajan, 2025c). It involves identifying critical data, assessing threats, analyzing weaknesses, and implementing countermeasures. It maintains the confidentiality of the information only to authorized users and detects any unusual behaviors that may expose malicious activities. It was originally developed by the US military during the Vietnam War to protect mission-critical information (Gentry & Gordon, 2019).

At present it is widely adopted across the business world to prevent data leaks, sabotage, and unauthorized access. The five steps of it are identifying critical information, analyzing threat, analyzing vulnerabilities, assessing risk, and applying countermeasures (D’Amore, 2022). It has access controls, risk management, vulnerability management, protective monitoring, incident management, configuration and change management, employee training, and monitoring activities to prevent data leaks and security breaches (Michnowicz, 2006). It is an analytical process that military, law enforcement, and government and private organizations use to prevent

sensitive or proprietary information from being accessed inappropriately (Athey, 2020).

*6.7 Mobile Security*

Mobile devices are smartphones, tablets, and laptops that are used not only to communicate, but also to plan and organize the works and lives. The technology evolves very rapidly, and the usages of mobile devices are increasing everyday life bringing various benefits, such as time savings, the ability to work without being tied to a specific position, and increased productivity. Mobile devices primarily contain access to corporate data, so businesses are highly prone to instant messaging attacks, phishing, and malicious apps (Rogers, 2013). People sometimes store sensitive information in mobile device, such as contacts lists, credit cards numbers, bank account number, passwords, and other important documents. Their chosen data are easily available on these devices, and attackers are focusing their efforts on mobile devices (Chan & Hong, 2016).

Mobile health (m-health) is the practices of public medical health supported by mobile technology that covers the collection, modification, classification, and transport of health-related data. Although basic telemonitoring m-health services are widely established, still there are difficulties to be resolved, most notably security and privacy concerns (Trigo et al, 2020). The mobile money (m-money) is revolutionizing the lives of vast unbanked population offering various benefits, such as simplicity, dependability, speed, flexibility, and cost. Rural areas and low-income persons can use the m-money system to get various services at a lower cost. This also reduces the security dangers associated with carrying real money, and reduces long queues at banking institutions (Ali et al., 2020).

Mobile security is the protection of mobile devices from threats through the use malicious apps, zero-day, phishing, and instant messaging attacks by the mobile computers and communication hardware (Bishop, 2004). Among the various types of cyber security, extended detection and response (XDR) is becoming an essential solution for modern enterprises that provides a unified approach to detect, respond, and mitigate threats (Engel et al, 2022).

*6.8 Zero Trust Security*

Actually zero trust is not about removing trust entirely so much as reducing it to the bare minimum necessary and making the trust explicit rather than implicit, and it involves understanding the traditional models it challenges. An operator implements a hard shell around his/her sensitive components. For example, a firewall around the data center can create castle walls, and entities outside the castle are potential threats requiring strict scrutiny, inside data are trusted and safe (KubeCrash, 2023). The conventional method of security is “trust but verify” it, but the zero trust paradigm adopts “never trust, always verify”, and the latter is significance due to various global cyber threats (Ranya & Goda, 2023).

Zero trust security is an IT security model that requires strict identity verification for every person, and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter. It assumes that there are attackers both within and outside of the network. It is implemented by establishing identity verification, validating device compliance prior to granting access, and ensuring least privilege access to only explicitly-authorized resources (Rose et al., 2020). It is better suited to modern IT environments than more traditional security approaches. It offers enterprises more network visibility and aids in the timely detection and mitigation of security threats. It assumes that all traffic and incoming data are malicious and need to check at every point-of-time (Pendli, 2025).

The term “zero trust” was coined by Stephen Paul Marsh in his doctoral thesis on computer security at the University of Stirling in April 1994, and later it is popularized by Forrester Research analyst John Kindervag in 2010 (Collier & Sarkis, 2021). Zero trust is a powerful security model that is at the forefront of modern security practices. Organizations are given the visibility and the employees require by zero trust privilege to guarantee ongoing compliance. A properly implemented zero trust privilege strategy can help the organizations to reduce the risk of breach by 50% (Guntaka, 2025).

*6.9 GenAI Security*

Generative AI (GenAI) has sparked a transformative wave across various domains, such as machine learning, healthcare, business, and entertainment due to its remarkable ability to generate lifelike data. GenAI products are ChatGPT and DALL E from openAI, Github Copilot, AlphaCode from Deepmind, etc. (Shoufan, 2023). It has become an essential pillar for organizations that aims to enhance productivity and innovation. It tempts business leaders to move quickly bypassing implications involving data, compliance, governance, and other risks (Bai et al., 2021).

The GenAI security is a newer type of cyber security that provides protection against the use and integration of securing GenAI applications and ecosystems. It prevents harmful actions, such as unauthorized data manipulation or misuse (Gupta et al., 2023). It encompasses all the measures, technologies, policies, and security

controls that protect organizations from risks associated with the use of GenAI. Some GenAI threats are model vulnerabilities, data risks, misuse scenarios, and compliance and governance risks (Golda et al., 2024).

GenAI security protects the entire lifecycle of GenAI applications from model development to deployment through the implementation of zero trust security, introduction of data protection measures, understanding of AI compliance obligations, and getting strong incident response plans in order (Jovanovic & Campbell, 2022). It helps to protect AI systems and their outputs from misuse, unauthorized access, and harmful manipulation. It improves threat detection, enhances operational efficiency, and personalizes security awareness training (Mohajan, 2025a). Several approaches are being employed to address the privacy and security concerns in GenAI, such as Privacy-Preserving Techniques (PPTs), Adversarial Defense Mechanisms, and Regulatory Measures and Policies (Wu et al., 2020).

*6.10 Secure Access Service Edge (SASE)*

A secure access service edge (SASE) is a new technology used to deliver wide area network and security controls as a cloud computing service directly to the source of connection rather than a data center (Kaur, 2024). It is the combination of security and networking elements offered in a single unified platform based on cloud-delivered services (Gareeb et al., 2021). It was first introduced by American research and advisory firm Gartner in 2019 as a response to the growing need for secure remote access and the increasing adoption of cloud-based services (Chen et al., 2023). The four key elements of security service edge (SSE) are Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), and Zero Trust Network Access (ZTNA) with SD-WAN capabilities, delivering them as a unified, cloud-native service (Makani, 2024). The SASE framework aims to provide a more agile, flexible, and scalable approach to network security (Joshi et al., 2021).

The SD-WAN is a key enabling technology for SASE that provides the necessary network connectivity and management capabilities. It enables organizations to create secure, high-performance connections between users, devices, and applications, across multiple locations and cloud environments (Gareeb et al., 2021). A Secure Web Gateway (SWG) is a security solution that protects users from web-based threats and enforces internet access policies, and acts as a first line of defense against malicious websites, phishing attempts, and other web-based attacks (Kaur et al., 2023). A Cloud Access Security Broker (CASB) is a security solution that acts as an intermediary between cloud service consumers and cloud service providers. It enforces security policies, monitor cloud activity, and protect sensitive data across multiple cloud platforms (Syed et al., 2022). Zero Trust Network Access (ZTNA) is a security model that operates on the principle of denying access by default, and treats all users, devices, and applications as untrusted until they are explicitly verified (Piplode & Singh, 2021). Firewall as a Service (FWaaS) delivers traditional firewall security features as a cloud-based service, and provides a scalable, flexible, and cost-effective alternative to on-premises firewall appliances, enabling organizations to protect their networks and applications from a wide range of threats (Walt & Venter, 2022).

*6.11 Operational Technology (OT) Security*

Operational technology (OT) causes a change through the direct monitoring and control of industrial equipment, assets, processes, and events that describes environments containing industrial control systems (ICS), such as supervisory control and data acquisition (SCADA) systems, distributed control system (DCS), remote terminal units (RTU) and programmable logic controllers (PLC), as well as dedicated networks and organization units (Koronios et al., 2010). The SCADA system provides centralized monitoring and control of complex processes spread across large areas that gathers real-time data from remote locations from sensors and instruments located at remote sites. It is widely used in industries, such as power generation, oil exploration, water management, manufacturing, etc. (Waqas & Jamil, 2024).

A Remote Terminal Unit (RTU) is an electronic device used in industrial and remote monitoring applications to collect data from sensors, process it, and transmit it to a central control system. It is essential for monitoring and controlling equipment and processes in geographically dispersed locations (Knapp, 2024). The PLC is a specialized industrial computer used to automate and control machinery and processes. That is designed to withstand harsh industrial environments and provides reliable operation over extended periods (Zaid & Garai, 2024).

As OT systems increasingly integrate with IT systems due to fourth industrial revolution initiatives, they become more vulnerable to cyber-attacks that pose risks not only to data but also to physical infrastructure (Kumar & Vardhana, 2025). The OT security refers to the cyber security practices and technologies that protect industrial systems controlling physical processes, ensuring the integrity, safety, and availability of critical infrastructure, such as power grids, utilities, healthcare, transportation networks, and manufacturing systems (Steenstrup, 2008). It focuses on safeguarding critical infrastructure from threats, such as malware, ransomware, and state-sponsored attacks, ensuring the continuity, safety, and reliability of essential operational services. It covers

security controls around process control systems (PCS), distributed control systems (DCS), and Scada environments that are collectively referred to as ICS environments (Kumar & Vardhana, 2025).

*6.12 Endpoint Security*

If a device, such as a desktop, a laptop, a tablet, a smartphone, etc. is connected to a network, such as a server, a database, an intranet, and an extranet; it is considered as an endpoint. That means endpoints can be plagued with both internal and external security threats. The term endpoint threat detection and response (ETDR) is coined by recognized security expert Anton Chuvakin in 2013 (Chuvakin, 2013). The vulnerabilities of endpoints seem endless and need strong security. Therefore, endpoint security is important at all levels of an organization and a company. It is the practice of securing endpoints of end-user devices, such as desktops, laptops, tablets, smartphones, smart printers, smart watches, ATM machines, and servers from being exploited by malicious actors and campaigns (Ahl, 2014). It is a cornerstone and critical component of effective cyber security frameworks due to hyper-connected digital landscape in an era of increasing cyber threats. It includes antivirus software, intrusion prevention systems (IPS), device encryption, and multi-factor authentication, and regular software updates. In many cases, threats are only detected after the loss of significant amounts of data (Fortinet, 2022).

Early approaches to endpoint security relied heavily on antivirus software and perimeter-based defenses. But the traditional endpoint protection platforms that focused on prevention are no longer enough to protect endpoints (Johnson et al., 2016). There are many antiviruses and anti-malware software scan and detect malicious software, such as viruses, worms, Trojans, and ransomwares (Forrester, 2021). As the volume and sophistication of cyber security threats have steadily grown, so has the need for more advanced endpoint security solutions that are designed to quickly detect, analyze, block, and contain attacks before they can do damage. Endpoint security is a continuous process that requires attention, resources, and preparation (ISC2, 2021). Firewalls are essential components of endpoint security that monitor and control incoming and outgoing network traffic, filtering out potentially malicious data packets (Slate, 2018). Keeping software and operating systems up to date with the latest security patches and updates is crucial for endpoint security. Recent studies emphasize the importance of adopting a multi-layered security approach that requires continuous verification of every device, user, and application accessing the network (Hanna et al., 2018). With endpoint security, companies and organizations can secure end-user devices, such as desktops and laptops with data and network security controls, advanced threat prevention, such as anti-phishing and anti-ransomware, and technologies that provide forensics, such as endpoint detection and response (EDR) solutions (ISC2, 2021).

## 7. Conclusions

At present, we are living in a world of cyber-format knowledge. We can send and receive any form of data, such as email, audio, and video without any leakage of information just by the click of a button due to cyber security. These data are maintained in the form of digital or cyber ways. Cyber security is an important field that is increasingly gaining attention as the internet and computer services are expanded. More efficient and effective cyber security is the responsibility of everyone and has the basics of confidentiality, integrity, and availability. Individuals and organizations must remain alert, adapt their security measures, and maintain a culture of security awareness to effectively mitigate risks in the cyber security.

## References

Ahl, I., (2014). The Relevance of Endpoint Security in Enterprise Networks. *Cyber-Development, CyberDemocracy and Cyber-Defense*, pp. 337-354. Springer, New York.

Alhassana, M. M., & Adjei-Quayeb, A., (2017). Information Security in an Organization. *International Journal of Computer*, *24*(1), 100-116.

Ali, G., et al., (2020). Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures. *Future Internet*, *12*(10), 160.

Andress, J., (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (2nd Ed.), Syngress.

Ang'udi, J. J., (2023). Security Challenges in Cloud Computing: A Comprehensive Analysis. *World Journal of Advanced Engineering Technology and Sciences*, *10*(02), 155-181.

Athey, P., (2020). *Are Phoneless Deployments the Future for Marines?* Defense News, November 16, 2020.

Babbie, E., (2009). *The Practice of Social Research* (12th Ed.). Belmont, CA: Wadsworth.

Bai, T., et al., (2021). AI-GAN: Attack-inspired Generation of Adversarial Examples. *2021 IEEE International Conference of Image Processing*, pp. 2543-2547. Publisher: EEE Computer Society, United States.

Baker, P., (2000). Writing a Literature Review. *The Marketing Review*, *1*(2), 219-247.

Belapure, S., & Godbole, N., (2011). *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*. Publisher: Wiley India.

Bishop, M., (2004). *Introduction to Computer Security*. Addison Wesley Professional.

Bolderston, A., (2008). Writing an Effective Literature Review. *Journal of Medical Imaging and Radiation Sciences*, *39*(2), 86-92.

Bryman, A., (2008). Of Methods and Methodology. *Qualitative Research in Organizations and Management*, *3*(2), 159-168.

Butt, U. A., et al., (2023). Cloud Security Threats and Solutions: A Survey. *Wireless Personal Communications*, *128*(1), 387-413.

Cabaj, K., et al., (2018). Cybersecurity: Trends, Issues, and Challenges. *EURASIP Journal on Information Security*, *2018*(1), 10.

Chahar, N. K., (2022). Computer Network Security. *International Journal of Innovative Science and Research Technology*, *7*(3), 1031-1034.

Chan, J. H., & Hong, J. L., (2016). Mobile Security and Its Application. *International Journal of Security and Its Applications*, *10*(10), 89-106.

Chandrasekaran, A. S., (2024). Demystifying Application Security: Keeping Applications Safe. *International Research Journal of Modernization in Engineering Technology and Science*, *6*(5), 6086-6095.

Chen, R., et al., (2023). Overview of the Development of Secure Access Service Edge. In *Signal and Information Processing, Networking and Computers, Lecture Notes in Electrical Engineering*, pp. 138-145.

Chuvakin, A., (2013). Named: Endpoint Threat Detection & Response. https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/

Collier, Z. A., & Sarkis, J., (2021). The Zero Trust Supply Chain: Managing Supply Chain Risk in the Absence of Trust. *International Journal of Production Research*, *59*(11), 3430-3445.

Creswell, J. W., (2013a). Review of the Literature. *Research Design. Qualitative, Quantitative, and Mixed Method Approaches* (4th Ed.). Thousand Oaks, California: Sage Publications.

Creswell, J. W., (2013b). *Qualitative Inquiry and Research Design: Choosing Among Five Traditions* (3rd Ed.). Thousand Oaks, California: Sage Publications.

D'amore, A. A., (2022). *Air Force Operations Security in the Twenty-first Century: An Unaddressed Vulnerability*. Wright Flyer Paper No. 87. Air University Press Maxwell Air Force Base, Alabama.

Daniel, K., & Titman, S., (2006). Market Reactions to Tangible and Intangible Information. *The Journal of Finance*, *61*(4), 1605-1643.

Danturthi, R. S., (2024). *Database and Application Security: A Practitioner's Guide*. Publisher: Addison-Wesley Professional.

Das, R., & Johnson, G., (2021). *Testing and Securing Web Applications*. Taylor & Francis Group, LLC.

Dhillon, G., (2007). *Principles of Information Systems Security: Text and Cases*. NY: John Wiley & Sons.

Dowd, P. W., & McHenry, J. T., (1998). Network Security: It's Time to Take It Seriously. *Computer*, *31*(9), 24-28.

Engel, M. M., et al., (2022). Mobile Device Security: A Systematic Literature Review on Research Trends, Methods and Datasets. *Journal of System and Management Sciences*, *12*(2), 66-78.

Erşahin, B., & Erşahin, M., (2022). Web Application Security. *South Florida Journal of Development*, *3*(4), 4194-4203.

Feruza, Y. S., & Kim, T., (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering*, *2*(2), 17-32.

Forrester, (2021). *Beyond Boundaries: The Future of Cybersecurity in the New World of Work*, September 2021. Cambridge, Massachusetts, USA.

Fortinet, (2022). *The Hidden Costs of Endpoint Security: Ransomware, Fileless Malware, and Management Issues*. White Paper. Sunnyvale, California, USA.

Gareeb, A. et al., (2021). Secure Access Service Edge (SASE): The Future of Network Security. *IEEE International Conference on Computing, Communication and Networking Technologies*, pp. 1-6.

Geneiatakis, D., et al., (2017). Security and Privacy Issues for an IoT Based Smart Home. 40th International

Convention on Information and Communication Technology, Electronics and Microelectronics, 22-26 May 2017, Opatija, Croatia, pp. 1292-1297.

Gentry, J. A., & Gordon, J. S., (2019). *Strategic Warning Intelligence: History, Challenges, and Prospects*. Washington, DC: Georgetown University Press.

Ghanad, A., (2023). An Overview of Quantitative Research Methods. *International Journal of Multidisciplinary Research and Analysis*, *6*(8), 3794-3808.

Ghansela, S., (2013). Network Security: Attacks, Tools and Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(6), 419-421.

Golda, A., et al., (2024). Privacy and Security Concerns in Generative AI: A Comprehensive Survey. *IEEE Access*, *12*, 48126-48144.

Goni, O., (2022). Cyber Crime and Its Classification. *International Journal of Electronics Engineering and Applications*, *10*(1), 1-17.

Groh, A., (2018). *Research Methods in Indigenous Contexts*. New York: Springer.

Guntaka, N. Y. R., (2025). Zero Trust and Cloud Identity: Building a Resilient Security Framework. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, *11*(1), 3450-346.

Gupta, G., et al., (2019). A Survey on Cloud Security Issues and Techniques. *International Journal on Computational Science & Applications*, *10*(9), 41-48.

Gupta, M., et al., (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access*, *11*, 80218-80245.

Hanna, S., et al., (2018). *IIC Endpoint Security Best Practices*. Industrial Internet Consortium, Object Management Group.

Hoffman, A., (2020). *Web Application Security: Exploitation and Countermeasures for Modern Web Applications* (1st Ed.). Publisher: O'Reilly Media, Inc.

Howell, K. E., (2013). *Introduction to the Philosophy of Methodology*. London, UK: Sage Publications.

Iqbal, H., et al., (2020). The Reality of Technologies for Cyber Security Challenges. *International Journal of Recent Technology and Engineering*, *9*(1), 2277-3878.

ISC2, (2021). A Resilient Cybersecurity Profession Charts the Path Forward. *Cybersecurity Workforce Study*, International Information System Security Certification Consortium (ISC2). Alexandria, Virginia, USA.

Johnson, C., et al., (2016). *Guide to Cyber Threat Information Sharing*. National Institute of Standards and Technology. US Department of Commerce.

Joshi, C., et al., (2017). Information Security Risks Management Framework: A Step towards Mitigating Security Risks in University Network. *Journal of Information Security and Applications*, *35*, 128-137.

Joshi, M., et al., (2021). Implementing Secure Access Service Edge (SASE): Best practices and considerations. *IEEE International Conference on Electronics, Computing and Communication Technologies*, pp. 1-6.

Jovanovic, M., & Campbell, M., (2022). Generative Artificial Intelligence: Trends and Prospects. *Computer*, *55*(10), 107-112.

Kalakuntla, R., et al., (2019). Cyber Security. *Holistica*, *10*(2), 115-128.

Kalsi, N., et al., (2023). IoT in Practice: Investigating the Benefits and Challenges of IoT Adoption for the Sustainability of the Hospitality Sector. *Computer Science & Information Technology*, *13*(13), 143-158.

Kaur, D., et al., (2023). Secure Web Gateway on Website in Cloud. In Big Data and Cloud Computing. *Lecture Notes in Electrical Engineering*, Springer.

Kaur, T., (2024). Secure Access Service Edge (SASE): Extending Network Security to Client. *International Journal of Innovative Research of Science, Engineering and Technology*, *13*(7), 13340-13347.

Knapp, E. D., (2024). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems* (3rd Ed.). Elsevier Inc.

Koronios, A., et al., (2010). Information and Operational Technologies Nexus for Asset Lifecycle Management. *Engineering Asset Lifecycle Management*, pp. 112-119, Springer, London.

Kramp, T., et al., (2013). Introduction to the Internet of Things. In *Enabling Things to Talk*, pp. 1-10. Springer, Berlin, Heidelberg.

Krawczyk-Sokołowska, I., & Caputa, W., (2023). Awareness of Network Security and Customer Value: The Company and Customer Perspective. *Technological Forecasting and Social Change*, *190*(1), 122430.

KubeCrash, (2023). *A Zero Trust Reference Architecture with Linkerd, Cert-manager, Emissary-ingress, and Polaris*. Ambassador, BUOYANT, Fairwinds, and Venafi.

Kumar, D., et al., (2018). Towards the Impact of Hacking on Cyber Security. *IIOABJ Journal*, *9*(2), 61-77.

Kumar, S., & Vardhana, H., (2025). *Cyber Security of OT Networks: A Tutorial and Overview*. arXiv:2502.14017v1 [cs.CR] 19 Feb 2025.

Kuzior, A., et al., (2024). Cybersecurity and Cybercrime: Current Trends and Threats. *Journal of International Studies*, *17*(2), 220-239.

Layton, T. P., (2007). *Information Security: Design, Implementation, Measurement, and Compliance*. Boca Raton, FL: Auerbach Publications.

Lehto, M., & Neittaanmäki, P., (2015). *Cyber Security: Analytics, Technology and Automation*. Springer International Publishing.

L'Esteve, R. C., (2023). New Horizons in Distributed Cloud Computing. In the *Cloud Leader's Handbook: Strategically Innovate, Transform, and Scale Organizations*, pp. 123-134. Berkeley, CA: Apress.

Li, X., & Xue, Y., (2011). *A Survey on Web Application Security*. Vanderbilt University, Nashville, TN.

Li, Y., & Liu, Q., (2021). A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments. *Energy Reports*, *7*(2021), 8176-8186.

Litoussi, M., et al., (2020). IoT Security: Challenges and Countermeasures. *Procedia Computer Science*, *177*(2020), 503-508.

Macfarlane, R., et al., (2012). Formal Security Policy Implementations in Network Firewalls. *Computers & Security*, *31*(2), 253-270.

Makani, S. T., (2024). Low-Cost, Self-Hosted Secure Access Service Edge (SASE) Solution Using AWS Cloud Infrastructure. *International Journal of Cyber Security*, *2*(1), 34-44.

Malallah, H. S., et al., (2023). Performance Analysis of Enterprise Cloud Computing: A Review. *Journal of Applied Science and Technology Trends*, *4*(1), 1-12.

Malik, J. A., et al., (2023). Empowering Cloud Security System with Blockchain Technology. *International Journal of Advanced Sciences and Computing*, *2*(1), 1-6.

McDonald, M., (2020). *Web Security for Developers*. No Starch Press, Inc.

Michnowicz, R. G., (2006). *OPSEC in the Information Age*. Strategy Research Project.

Miorandi, D., et al., (2012). Internet of Things: Vision, Applications and Research Challenges. *Ad Hoc Networks*, *10*(7), 1497-1516.

Mohajan, H. K., (2017). Two Criteria for Good Measurements in Research: Validity and Reliability. *Annals of Spiru Haret University Economic Series*, *17*(3), 58-82.

Mohajan, H. K., (2018a). Aspects of Mathematical Economics, Social Choice and Game Theory. PhD Dissertation. University of Chittagong, Chittagong, Bangladesh.

Mohajan, H. K., (2018b). Qualitative Research Methodology in Social Sciences and Theoretical Economics. *Journal of Economic Development, Environment and People*, *7*(1), 23-48.

Mohajan, H. K., (2020). Quantitative Research: A Successful Investigation in Natural and Social Sciences. *Journal of Economic Development, Environment and People*, *9*(4), 50-79.

Mohajan, H. K., (2025a). Artificial Intelligence: Prospects and Challenges in Future Progression. *Art and Society*, *4*(7), 38-50.

Mohajan, H. K., (2025b). Machine Learning: A Brief Review for the Beginners. Unpublished Manuscript.

Mohajan, H. K., (2025c). Deep Learning: A Brief Study on Its Architectures and Applications. Unpublished Manuscript.

Mohajan, H. K., (2025d). Cybercrime: A Potential Threat to Global Community. Unpublished Manuscript.

Mondal, A., et al., (2020). Cloud Computing Security Issues & Challenges: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering*, *8*(1), 60.

Moore, R., (2005). *Cyber Crime: Investigating High-Technology Computer Crime*. Cleveland, Mississippi: Anderson Publishing.

Mouna, B., & Yassine, M., (2024). Business Leadership in E-Commerce in the USA: The Impact of Block-chain Technology. *Business Ethics and Leadership*, *8*(1), 116-128.

Murphy, C., (2024). *Understanding Cybercrime*. European Parliamentary Research Service, European Parliament.

Nabi, M. N., & Islam, M. T., (2023). Cyber Security in the Globalized World: Challenges for Bangladesh. Conference: *Economic and Social Development*. 7th International Scientific Conference, New York, USA.

Najar, A. H., (2019). Internet of Things (IoT): Security Issues and Challenges. *International journal of Management, IT and Engineering*, *9*(3), 248-260.

Patnaik, P. C., (2021). Network Security: Concepts and Various Aspects for Treating the Attacks. *International Journal of Scientific Development and Research*, *6*(2), 396-400.

Paul, P. K., & Aithal, P. S., (2019). Cloud Security: An Overview and Current Trend. *International Journal of Applied Engineering and Management Letters*, *3*(2), 53-58.

Pawar, M. V., & Anuradha J., (2015). Network Security and Types of Attacks in Network. *Procedia Computer Science*, *48*(2015), 503-506.

Pendli, N. R., (2025). Blockchain for Zero-Trust Security Models: A Decentralized Approach to Enterprise Cybersecurity. *Journal of Information Systems Engineering & Management*, *10*(33s), 807-813.

Piplode, S., & Singh, U. K., (2021). An Overview of Cloud-Based Firewall for Network Security. *International Journal of Scientific Research in Science Engineering and Technology*, *8*(5), 113-152

Rajendran, S., (2015). *Mobile Application Security with Open-Source Tools*. Philips India Limited.

Ranya, V., & Goda, R., (2023). *Zero Trust Framework "Don't Trust, Verify First"*. Dell Technologies, Dell Inc.

Rao, T. A., & Haq, E. U., (2018). Security challenges facing IoT layers and its protective measures. *International Journal of Computer Applications*, *179*(27), 31-35.

Reese, G., (2009). *Cloud Application Architectures: Building Applications and Infrastructure in the Cloud*. O'Reilly Media, Inc., Sebastopol, USA.

Reid, R., & van Niekerk, J., (2014). From Information Security to Cyber Security Cultures Organizations to Societies. *Information Security South Africa* (ISSA), Johannesburg, South Africa.

Rittinghouse, J. W., & Ransome, J. F., (2009). *Cloud Computing: Implementation, Management and Security*. CRC Press, Taylor & Francis Group, Boca Raton.

Rogers, D., (2013). *Mobile Security: A Guide for Users*. Copper Horse Solutions Limited.

Rose, S., et al., (2020). *Zero Trust Architecture. National Institute of Standards and Technology*. Special Publication 800-207. US Department of Commerce.

Said, Z. M., & Zolkipli, M. F., (2022). Internet of Things (IoT): A Study of Security Issues and Challenges. *International Journal of Recent Contributions from Engineering Science & IT*, *10*(2), 16-31.

Sang, N. T., & Trung, B. B., (2022). Cybercrime in the Digital Age: Challenges and Implication for Prevention. *International Journal of Social Science and Human Research*, *5*(11), 5082-5086.

Santos, O., (2020). *Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide (Certification Guide)*. Cisco Press.

Schmidt, N., (2014). Critical Comments on Current Research Agenda in Cyber Security. *Obrana a Strategie*, *14*(1), 29-38.

Seifert, M., et al., (2023). Hybrid Clouds Arising from Software as a Service Adoption: Challenges, Solutions, and Future Research Directions. *ACM Computing Surveys*, *55*(11), 1-35.

Shahidullah, S., et al. (Eds.), (2022). *Global Cybercrime and Cybersecurity Laws and Regulations: Issues and Challenges in the 21st Century*. Nova Science Publishers Inc.

Shields, P. M., & Rangarjan, N., (2013). *A Playbook for Research Methods: Integrating Conceptual Frameworks and Project Management*. Stillwater, OK: New Forums Press.

Shin, Y., & Williams, L., (2008). An Empirical Model to Predict Security Vulnerabilities Using Code Complexity Metrics. *Proceedings of the Second International Symposium on Empirical Software Engineering and Measurement*, ESEM 2008, October 9-10, 2008, Kaiserslautern, Germany, pp. 315-317.

Shoufan, A., (2023). Exploring Students' Perceptions of ChatGPT: Thematic Analysis and Follow-up Survey. *IEEE Access*, *11*, 38805-38818.

Shuaibu, B. M. et al., (2013). Systematic Review of Web Application Security Development Model. *Artificial Intelligence Review*, *43*(2), 259-276.

Singh, A., & Chatterjee, K., (2017). Cloud Security Issues and Challenges: A Survey. *Journal of Network and Computer Applications*, *79*(2017), 88-115.

Sisaneci, I., et al., (2013). A Novel Concept for Cybersecurity: Institutional Cybersecurity. The 6th International Conference on Information Security and Cryptology, Turkey, Ankara, Sep. 20-21, 2013.

Slate, S., (2018). Endpoint Security: An Overview and a Look into the Future. 7 May, 2018.

Srinivasan, M. K., et al., (2012). *State-of-the-art Cloud Computing Security Taxonomies*. Proceedings of the International Conference on Advances in Computing, Communications and Informatics ICACCI '12. pp. 470-476.

Steenstrup, K., (2008). IT and OT: Intersection & Collaboration. *Gartner Industry Research*, ID No G00161537, USA.

Susanto, H., & Almunawar, M. N., (2022). *Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standards*. Publisher: Francis and Taylor.

Syed, N., et al., (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, *10*(3), 57143-57179.

Taherdoost, H., (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, *215*(2022), 483-487.

Tawalbeh, L. A., et al., (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, *10*(12), 4102.

Torraco, R. J., (2016). Writing Integrative Literature Reviews: Using the Past and Present to Explore the Future. *Human Resource Development Review*, *15*(4), 404-428.

Trigo, J. D., et al., (2020). Building Standardized and Secure Mobile Health Services Based on Social Media. *MDPI Electronics*, *9*(12), 2208.

Velev, D., & Zlateva, P., (2011). Cloud Infrastructure Security. Open Research Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2010, Sofia, Bulgaria, March 5-6, 2010.

Vick, A. J., (2015). *Air Base Attacks and Defensive Counters: Historical Lessons and Future Challenges*. Santa Monica, CA: RAND Corporation.

Walt, S. & Venter, H., (2022). Research Gaps and Opportunities for Secure Access Service Edge. *International Conference on Cyber Warfare and Security*, 17, pp. 609-619.

Wendy, & Wang, G., (2019). Measuring Information Security and Cybersecurity on Private Cloud Computing. *Journal of Theoretical and Applied Information Technology*, *96*(1), 156-168.

Wu, N., et al., (2020). A Privacy-Preserving Game Model for Local Differential Privacy by Using Information-Theoretic Approach. *IEEE Access*, 8, 216741-216751.

Zaid, T. & Garai, S., (2024). Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers. *Blockchain in Healthcare Today*, *7*(1), 302.

Ziegeldorf, J. H., et al., (2014). Privacy in the Internet of Things: Threats and Challenges. *Security and Communication Networks*, *7*(12), 2728-2742.

**Copyrights**