

A REVIEW: PROTECTING DIGITAL INFRASTRUCTURE IN CYBER SECURITY USING ARTIFICIAL INTELLIGENCE

Tanveer Baig Z Lecturer¹, Nodira Rakhimkhodjaeva²

¹Management Development Institute of Singapore in Tashkent

²Dean Undergraduate Studies Management Development Institute of Singapore in Tashkent

Abstract— The internet is now recognized as perhaps the most powerful media that has affected various aspects of people's life, including the working process. Since various operations in people's lives including financial, social, and others involve online systems there has been a rise in cyber threats. In this article, the author discusses multiple types of cyber threats, including phishing, ransomware, malware, and suggests ways to avoid cyber threats for regular users. Moreover, it focuses on measures conducted on the international level to address the problem of cyber-guarantee while highlighting trends and events concerning the appreciation of cybersecurity in Uzbekistan. Fortunately, this article includes numerous relevant examples and show that it is necessary to remain cautious and informed about cybersecurity measures in order to protect our personal information from rapidly growing cyber threats

Keywords: Cybersecurity, Threats, Phishing, Cybersecurity Trends, Artificial Intelligence in Cybersecurity, Machine Learning Security.

I. INTRODUCTION

The importance of the internet in people's lives has increased greatly over the last twenty years. Internet is now an indispensable part of modern life, including purchases and payments, communication, social networks and remote work. As useful as it is and as much as it improves the chances of communication, the internet also comes with great risks significantly the risk of cyberattacks. Some of the cyber threats are as follows:– Phishing, ransomware, identity thefts, data breaches, and others are continuously changing in Their nature. In such environment one has to be very cautious and alert in order to protect own organization and personal assets from being hacked.

To achieve these objectives, this article seeks to understand the various types of cyber threats; how people can protect themselves from such risks and various ongoing efforts all over the world to regulate cyber risks. Furthermore, it narrates personal experiences & ideas on rising demand of

cybersecurity all over the globe with focus to Uzbekistan where, the knowledge of cybercrime is now gradually gaining traction.

1.1 Need for Cybersecurity

Cybersecurity is defined as the safeguarding of systems, networks, and data against cyber threats and unauthorized access. It involves a comprehensive array of practices and technologies aimed at defending digital infrastructures from cybercriminals, hackers, and other malicious entities. As technological advancements progress, the tactics employed by adversaries to breach systems and compromise sensitive information also become more sophisticated. Consequently, cybersecurity is a dynamic field that necessitates ongoing adaptation and vigilance.

At its foundation, cybersecurity is structured around the CIA Triad, which consists of:

Confidentiality: Ensuring that sensitive information is accessible only to authorized personnel.

Integrity: Maintaining the accuracy and unaltered state of data.

Availability: Guaranteeing that systems and data are reachable when required by authorized users.

These fundamental principles assist organizations and individuals in establishing secure digital environments and reducing the likelihood of data breaches or system vulnerabilities.

1.2 Types of Cyberattacks

Cyberattacks manifest in various forms, each targeting specific vulnerabilities within digital systems. Recognizing these prevalent attack types is essential for effective defense strategies. Below are some of the most common cyber threats.

a. Phishing Attacks

Phishing represents one of the most widespread types of cyberattacks. This form of social engineering involves criminals masquerading as legitimate organizations or trusted individuals to obtain sensitive information, including usernames, passwords, or financial data. Phishing typically occurs through emails, text messages, or phone calls. The attacker may dispatch a communication that seems to originate from a credible source, such as a financial institution or government body, prompting the recipient to verify their account details or undertake an action that directs them to a fraudulent website.

Real-Life Example:

A friend of mine received an email that seemed to come from his bank, alerting him that his account had been compromised. The email contained a link to a "secure" website where he was

prompted to enter his login credentials. After following the link and entering his information, his account was drained by cybercriminals. The email had a convincing design, mimicking the bank's real communication.

Preventions

- Never trust unsolicited messages that ask for personal information.
- Always verify the source of the communication, especially if the request is urgent or seems suspicious.
- Use multi-factor authentication (MFA) to add an extra layer of security to your accounts.

b. Link-Based Attacks

These attacks typically occur through social media platforms, messaging apps, or email. The attacker may send a link to a victim, claiming it leads to a useful resource or important information. However, when the victim clicks on the link, they are redirected to a malicious website or unknowingly download malware onto their device.

Personal Experience:

I once received a message on Telegram from someone who appeared to be a close friend. The message contained a link to an "interesting" article. However, when I clicked on it, my account was hijacked, and the hacker began sending spam messages to my contacts. The hacker had used a compromised version of my own account to deceive others into clicking the link.

How to Protect Yourself:

- Verify the authenticity of links before clicking on them, especially when sent by people you don't frequently communicate with.
- Use security tools that can detect malicious links or redirect you away from dangerous websites.
- Be cautious with shortened URLs or links that seem unfamiliar.

c. Ransomware

Ransomware represents a type of malware that encrypts a victim's files or denies them access to their system, requiring a ransom payment to regain access. Ransomware attacks frequently target companies, hospitals, or governmental bodies but also affect individuals.

Ransomware can spread through malicious email attachments, infected software, or compromised websites. The financial and operational damage caused by ransomware attacks can be

devastating.

How to Protect Yourself:

- Regularly back up your files to minimize the impact of a ransomware attack.
- Be cautious about downloading files from untrusted sources or opening attachments in unsolicited emails.
- Keep your software up to date, as patches and updates often address vulnerabilities that ransomware can exploit.

d. Malware

Malware encompasses a wide array of malicious software intended to infiltrate and harm computers, networks, or systems. Malware can consist of viruses, worms, Trojans, and spyware. It is commonly distributed through infected email attachments, harmful websites, or pirated software downloads.

How to Protect Yourself:

- Install and update antivirus software regularly to detect and block malware.
- Avoid downloading files from unknown or untrusted sources.
- Keep your operating system and other software updated to patch security vulnerabilities.

II. REVIEW OF LITERATURE

This section we have collected various research article which mainly focused on cyber attacks and its solutions. A cyber security assessment model constructed using a Random Neural Network is able to identify issues as well as strengthen the mechanism of protecting the IoT devices against attacks [1]. Real Time traffic analysis of the devices improves the sequential learning approach to identify IoT devices that were compromised during a botnet attack [2].

There exists an online framework of deep learning which is self supervised to improve the effectiveness and flexibility of intrusion detection systems in complex environments [3]. The paper scrutinizes the vulnerabilities and trust models in communication systems which have multi components with a focus in the strength and security of the systems in regard to interactions. [4]. There is a distributed federated intrusion detection framework that has been developed for Health IoT and Internet of Vehicles to improve security in this areas [5]. New and developing age impacts, problems and development strategies in the principles of cyber security practice [6]. There is a necessity for changing the approach taken to connect different devices in order to cater for cybersecurity issues present in future help systems [7]. Cyber vulnerabilities and security techniques

that will enhance resilience and reliability of the IoE systems from being malicious hacked [8]. Multi-layered approaches of making any cyber electronic power system more secure [9]. AI tools especially focused on malware detection and intrusion prevention for smart infrastructures and industrial systems protection.[10].The cybersecurity simulation platform is being developed for training and testing security measures of the critical infrastructure systems. [11].Emerging threats in the cybersecurity landscape and emphasizes new technologies that can counter these threats in different areas.[12].Self-organizing networks that are able to continuously maintain real-time security, service quality, and energy consumption at acceptable levels.[13].Ways to reduce energy consumption and increase the computational efficiency of software applications with a long run-time.[14].The trade-offs and interdependencies that exist between energy efficiency, reliability, security, and maintenance in computer networks.[15-19].

III. CASE STUDIES ON THE CYBER SECURITY ATTACKS ALL OVER THE WORLD AND ITS SOLUTIONS

IV. Global Cybersecurity Efforts

Economic Impact of Cybercrime (2015-2024)

A line graph showing the increasing economic damage caused by cybercrime globally, demonstrating the financial strain on organizations. As shown in fig 1

Graph Title: Global Economic Impact of Cybercrime (2015-2024) Year (2015 to 2024)
Economic Losses (in trillion USD)

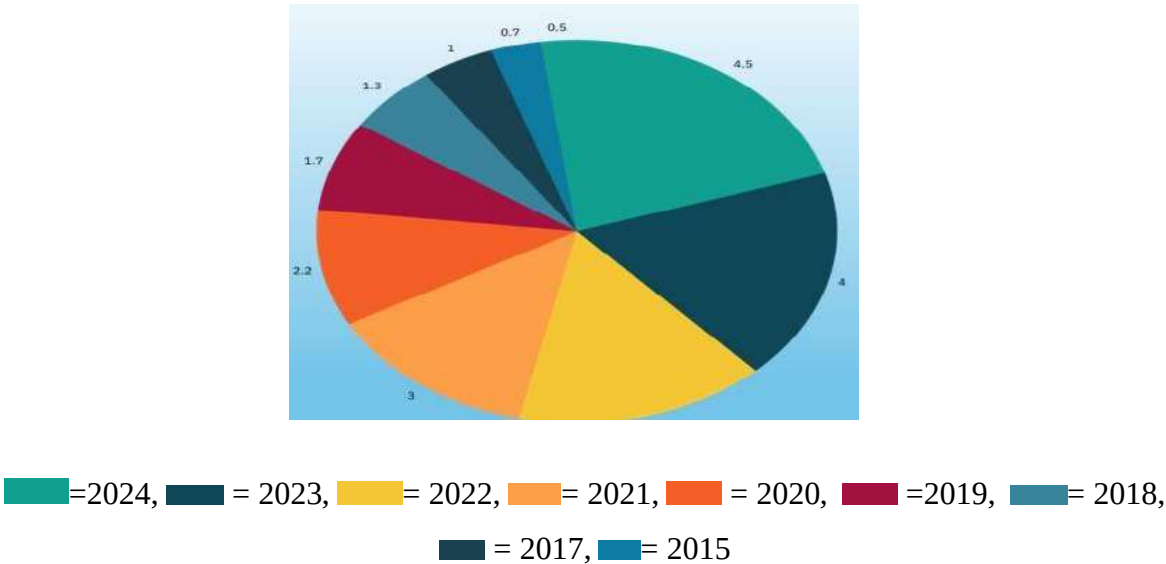


Fig 1: Global Economic Impact of Cybercrime (2015-2024)

Cyberattack threat level (1 to 4) for banks in Europe in 2024

Rising Cybercrime Costs: The cost of cybercrime is projected to reach \$9.5 trillion in 2024,

tripling since 2015. This escalation emphasizes the critical need for robust cybersecurity strategies across all sectors, especially in finance. Increased Cybersecurity Budgets: In response to growing threats, organizations are boosting their cybersecurity budgets. For example, the U.S. government allocated \$13 billion for IT security, reflecting a commitment to combating cyber threats. As

The data from 2024 underscores the persistent and evolving nature of cyber threats facing the banking industry worldwide. Financial institutions must continue to adapt and enhance their cybersecurity measures to protect against increasingly sophisticated cyberattacks as shown in fig 2

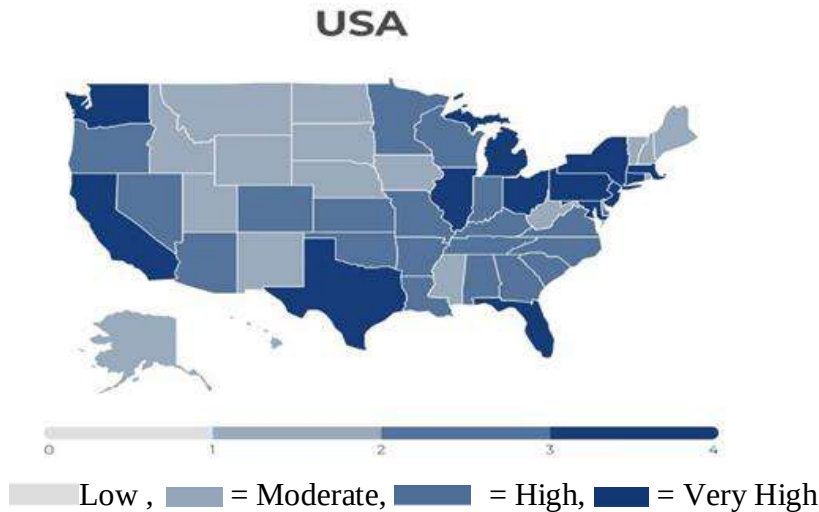


Fig 2 : Map of USA depicting the case of cyber-attacks from Low to High

Data Breaches: The U.S. experienced substantial data breaches in its financial sector. Notably, LoanDepot, a major mortgage lender, reported a breach affecting 16.9 million customers, exposing sensitive information such as names, addresses, and financial account numbers.

Ransomware Attacks: Ransomware remained a prevalent threat, with 66% of organizations affected in 2023, leading into 2024. The financial impact of these attacks was significant, with data breaches costing businesses an average of \$4.88 million as shown in fig 3

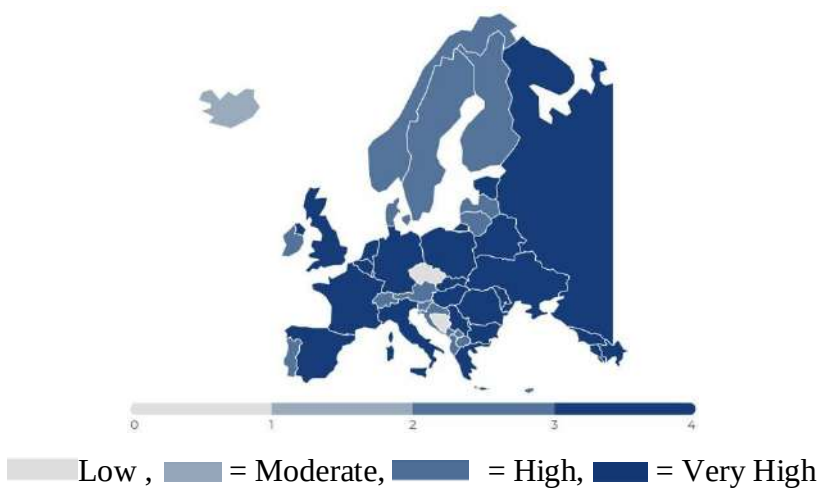


Fig 3: Map of Europe depicting the case of cyber-attacks from Low to High

Breakdown of Cybersecurity Threats by Industry (2024)

This chart would show the percentage distribution of cyberattacks by various sectors, emphasizing financial institutions as the most targeted as shown below fig 4

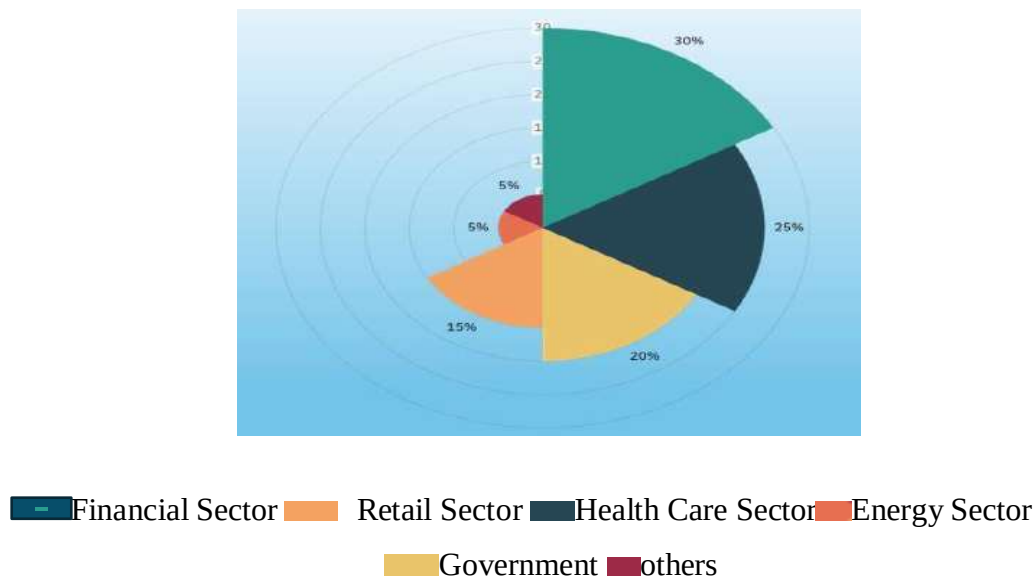


Fig 4: : Breakdown of Cybersecurity Threats by Industry (2024)

Advent of New Cyber Threats: A DDOS attack occurred on UK businesses every 44 seconds in the year examined which is 5% more than the previous year. This escalation highlights the risk of increasing the cyber attack threat landscape in the UK exponentially.

Concerns Related to Financial Sector: Cybersecurity was the most widely reported risk of concern amongst global banks with 72% of and Chief Risk Officers declaring it as such. This goes to show that there is an increasing sense and more allocating of resources towards cybersecurity in the UK financial sector. The case studies of the Asian countries are listed below

China:

Ransomware Incidents: The banks in China weren't spared from the ransomware attacks. The Industrial and Commercial Bank of China (ICBC) is one of the banks that got affected which shows how cybercriminals operate from a global perspective.

Espionage Activities: Hackers working for China also called Salt Typhoon seem to have breached several US telecommunications providers and many other providers in more than 20 countries which means they possess cyber skills that can be deployed in the financial sectors across the world.

Thailand:

Cybersecurity Challenges: The banking industry in Thailand reported an escalation in cyberattacks, which included a marked rise in attempts to compromise customer accounts by means of phishing. In relation to the past year, the Bank of Thailand indicated a 30% rise in instances of

cyber incidents.

Singapore:

Advanced Persistent Threats (APTs): APT groups that employ complex malware to attack systems targeted Singaporean banks. The Monetary Authority of Singapore (MAS) sought to curb such risks by issuance of advisories increasing the level of cyber threat in the country.

India:

Data Breaches: Indian banks recorded embarrassing security breaches with more than 1.3 million debit and credit card data, which compromised security accounts, being dumped on the dark web. To avoid such risks in the future, the Reserve Bank of India (RBI) required security measures to be increased.

v. CYBERATTACK THREAT LEVEL (1 TO 4) FOR BANKS IN ASIA IN 2024

Rising Cybercrime Costs: The cost of cybercrime is projected to reach \$9.5 trillion in 2024, tripling since 2015. This escalation emphasizes the critical need for robust cybersecurity strategies across all sectors, especially in finance as shown in fig 5

Increased Cybersecurity Budgets: In response to growing threats, organizations are boosting their cybersecurity budgets. For example, the U.S. government allocated \$13 billion for IT security, reflecting a commitment to combating cyber threats.

The data from 2024 underscores the persistent and evolving nature of cyber threats facing the banking industry worldwide. Financial institutions must continue to adapt and enhance their cybersecurity measures to protect against increasingly sophisticated cyberattacks.

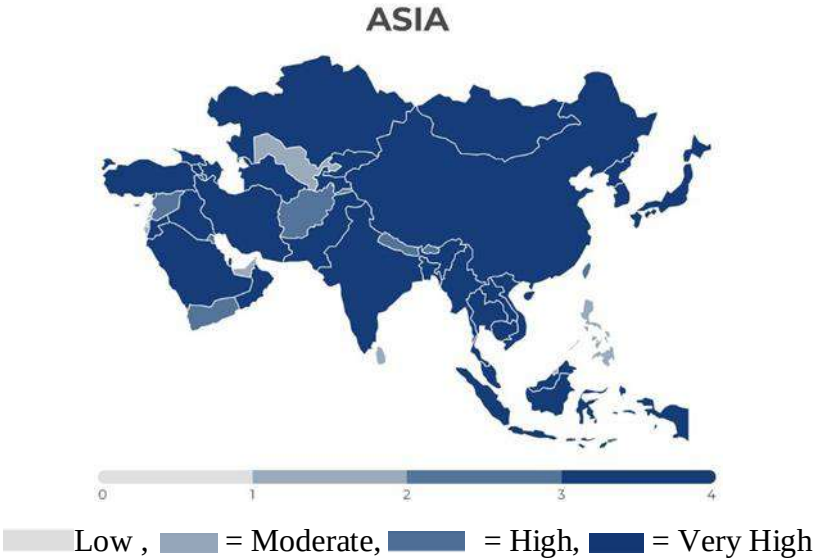


Fig 5 : Map of Asia depicting the case of cyber-attacks from Low to High

Uzbekistan:

Emerging Threat Landscape: During its growth, the banking industry of Uzbekistan encountered a range of cyber threats especially targeting phishing and malware challenges for mass

financial cases. The Central Bank of Uzbekistan carried out campaigns on the promotion of cyberspace protection against phishing and malware for the institutions and the customers.

In Uzbekistan, the internet has become a vital part of daily life, but the risks of cyberattacks have increased. In response, the government has introduced several measures to combat cybercrime, such as awareness programs aimed at older adults, who are often more susceptible to scams like phishing.

Personal Experience in Uzbekistan:

I once encountered a phishing scam through Telegram, where my account was compromised after I clicked on a fraudulent link. This experience highlighted the urgent need for cybersecurity education, particularly in Uzbekistan, where many people are still unfamiliar with common cyber threats.

VI. RESULT AND DISCUSSION

The Need for Cybersecurity Education in Schools

In my opinion, every high school should include cybersecurity in its curriculum. As more young people become internet users, it is essential to educate them about the risks associated with online activities and how to protect themselves. This education should cover basic topics such as recognizing phishing emails, using strong passwords, and understanding the importance of software updates and security tools.

Practical Steps for Everyday Protection

- Utilize Robust, Distinct Passwords: Formulate intricate passwords that incorporate a combination of uppercase letters, lowercase letters, numerals, and special characters. Steer clear of commonly used passwords and refrain from reusing passwords across different accounts.

- Activate Two-Factor Authentication (2FA): Whenever feasible, implement 2FA to enhance the security of your accounts with an additional protective layer.

Exercise Caution with Personal Information: Remain vigilant regarding the details you disclose online. Limit the amount of personal information shared on social media platforms, as excessive sharing can render you vulnerable to cybercriminals.

- Authenticate Unknown Links and Emails: Always verify the legitimacy of links and emails, particularly those requesting personal information. If uncertain, reach out to the sender directly for confirmation.

VII. FUTURE SCOPE

We cannot pick up a newspaper these days without reading an account of a data breach resulting in cyber fraud or theft. This has a particularly negative effect on corporate stakeholders because they may suffer reputational damage and the loss of privacy. Investors who are ready to invest in the organization also suffer. Cyber protection is now an area which is economically significant. What are

the various chances and directions of development for the field of cyber security in the coming years? Let's have a look at the trends that the cyber security industry is likely to witness in the next few years.

Artificial Intelligence and Machine Learning Integration:

Advanced machine learning algorithms and artificial intelligence tools are bound to change the nature of the organization's ability to cultivate cyber resilience. Incorporating these technologies into procedures will help organizations prepare for cyber threats before they become a major concern or risk.

Cybersecurity in IoT (Internet of Things):

Although this concern is to be commonly raised in the future, it is expected that IoT security will require strong attention. Protecting these devices, as use and penetration of IoT devices across industries grows will become critical. Future research requirements will emphasize the development of good IoT architectures which will be able to combat emerging cyber attacks.

Cyber Protection Strategy on Secure SDLC:

Considering the ever-present IoT security issues for the widespread use of the Internet of Things throughout all industries. The cynosure will be on the development of more effective cybersecurity approaches and procedures.

Blockchain for Cybersecurity:

Blockchain technology provides a the ability to create a file, information ordt transaction that can be accessed from multiple locations, thus portraying a fail-safe system against tampering or alteration of any information contained in the blockchain ledger. Future use of blockchain in cyber security could see the development of advanced systems for managing identity and impersonation detection and prevention.

Quantum Computing and Cyber Security:

The emergence of quantum computing opens up possibilities as well as threats for cybersecurity. On one hand, the advances in quantum algorithms could have negative implications for different types of encryption methodology, but nevertheless, quantum technologies could bring more advanced ways of encryption.

Cyber Security Education and Awareness programs:

The national as well as the global cyberspace awareness divide is still a challenge to many countries across the globe. Future campaigns are likely to target embedding cyber security as part of the school mainstream education and providing affordable awareness programs that cut across all ages.

Fantasy of the World with Cyber Security:

The journey of Cyber attacks Commences over borders which necessitate globalization. Risk

mitigation International Partnerships (which come from the effort of empathy), commonly agreed upon protocols and knowledge of dissolution determinants would be signature in the future cyber security frameworks.

Concentration on Advocacies Regimes for data Privacy Protection Requirements and Compliance Obligations: Government spheres across the globe are expected to soften their most say to treaties conversation around data privacy treaties and online protection compliance obligations. Such measures will ensure businesses be answerable in guarding clients' personal information.

Strengthened Cybersecurity in Financial Entities:

The digitization of financial systems is on the rise, the systems which includes, attempting to prevent cyber robbery and wire frauds including the integration of other mechanisms in the banking systems and financial technology, will continue to advance.

Dissolution of the Threat of Cyber Warfare initiated by the Government:

In view of government sponsored cyber wars that are on the increase, advanced systems need of governments and private organizations are able to defend such kind of politically motivated cyber attacks.

Finally, cyber security will have include all the violence including technology violence, international violence, regulation violence and education violence. Such action should help in creating a robust strong internet environment which will be able to combat the challenges of the future cyber world.

VIII. **CONCLUSION**

As the digital landscape continues to advance and permeate various facets of our existence, the importance of cybersecurity will only intensify. Cyberattacks are inevitable, making it crucial to adopt a proactive stance in safeguarding our online presence. By enhancing our understanding of prevalent cyber threats, we can diminish the chances of becoming victims of such attacks. It is imperative that governments, educational institutions, and individuals collaborate to cultivate a more secure digital environment. Cybersecurity transcends mere technical concerns; it is a societal challenge that necessitates collective awareness, education, and action.

REFERENCES

- [1] E. Gelenbe and M. Nakip, "Traffic Based Sequential Learning During Botnet Attacks to Identify Compromised IoT Devices," IEEE Access, 2022.
- [2] M. Nakip and E. Gelenbe, "Online Self-Supervised Deep Learning for Intrusion Detection Systems," IEEE Transactions on Information Forensics and Security, 2024.
- [3] E. Gelenbe, M. Nakip, and M. Siavvas, "System Wide Vulnerability and Trust in Multi-Component Communication System Software," to be published in IEEE Network, 2024.

- [4] E. Gelenbe, B. C. Gül, and M. Nakip, "DISFIDA: Distributed Self-Supervised Federated Intrusion Detection Algorithm with Online Learning for Health Internet of Things and Internet of Vehicles," to be published in Internet of Things, December 2024.
- [5] T. Vartiainen et al., "Development of Cybersecurity Simulator-Based Platform for the Protection of Critical Infrastructures," 2024.
- [6] IBM Security, "The Role of AI in Cybersecurity: Trends and Insights." Available: <https://www.ibm.com/security>. [Accessed: June 24, 2024]
- [7] National Institute of Standards and Technology (NIST), "Zero Trust Architecture (SP 800-207)." Available: <https://www.nist.gov>. [Accessed: June 24, 2024].
- [8] European Union Agency for Cybersecurity (ENISA), "Cybersecurity Skills and Workforce Development." Available: <https://www.enisa.europa.eu>. [Accessed: June 24, 2024].
- [9] McKinsey & Company, "Cybersecurity in Financial Services: Building Digital Trust." Available: <https://www.mckinsey.com>. [Accessed: June 24, 2024].
- [10] CM Alliance, "Biggest Cyber Attacks, Data Breaches, and Ransomware Attacks in 2024." Available: <https://www.cm-alliance.com/cybersecurity-blog/may-2024-biggest-cyber-attacks-data-breaches-ransomware-attacks>.
- [11] PwC, "2024 Global Digital Trust Insights." Available: <https://www.pwc.com/bm/en/press-releases/pwc-2024-global-digital-trust-insights.html>. [Accessed: June 24, 2024].
- [12] E. Gelenbe and M. Nakip, "IoT Network Cybersecurity Assessment With the Associated Random Neural Network," IEEE Access, 2023.
- [13] "Cyber Security Challenges and Trends on Recent Technologies," presented at an IEEE conference, 2022.
- [14] "Cybersecurity for Next-Generation Connectivity Systems—Rethinking Architecture," IEEE Communications Standards Magazine, 2022.
- [15] "Future Security Issues in Internet of Energy," IEEE Xplore, 2023.
- [16] K. Gupta, S. Sahoo, and B. K. Panigrahi, "A Monolithic Cybersecurity Architecture for Power Electronic Systems," 2024.
- [17] M. Schmitt, "Securing the Digital World: Protecting Smart Infrastructures and Digital Industries with AI-Enabled Malware and Intrusion Detection," 2023.
- [18] Tanveer Baig and Ather, Danish and Setia, Sonia and Quraishi, Suhail Javed and , and Mian, Syed Mohtashim", "Towards Advanced Animal Care: A Li-Fi and IoT-Based System for Monitoring Newborn Livestock", journal="ES Materials & Manufacturing", issn="2576-9898", doi="10.30919/esmm1038.
- [19] Danish Ather, ,Tanveer Baig .Z, Ambuj Kumar Agarwal, Suhail Javed Quraishi ,Malikhan singh ,Rajeesh, "Integrating Internet of Things Sensors with Machine Learning forUrinary Tract Infection Prediction in Male Felines ” KherlJournal of Intelligent Systems and Internet of ThingsVol. 14, No. 01, PP. 265-277, 2025DOI: <https://doi.org/10.54216/JISIoT.140121>