Study on cybersecurity-: Trending Challenges, Emerging Trends, and threats.

Rabban Javed,
AIIT, Amity University
Noida, Uttar Pradesh, India
rabban.javed@s.amity.edu

Dr. Rashmi Vashisht,
Amity University,
Noida, Uttar Pradesh, India
rvashisth@amity.edu

Nidhi Sindhwani
Amity University,
Noida, Uttar Pradesh, India
nsindhwani@@amity.edu

l. ABSTRACT

A. Background:

Due to the growth in cyber threats such as hacking, phishing, virus assaults, and identity theft, cybersecurity has developed over time. Governments, companies, and people have all made significant investments in cybersecurity measures to safeguard their private data from hackers.

Computer technology is being used to modernize the world's power grids, not an exception is India. The power grid performance of India has been improved due to the growing use of computers and computer systems, but it has also presented new difficulties. Devices for digital monitoring, protection, and metering are highly connected to the internet. As a result, cybercriminals may now have their sights set on the Indian Grid. [1].

Keywords: Cyber-security, Risk, Security, Cyber-attacks, challenges, Cyber-threats, and trends.

B. Significance of the research

Governments, organizations, and people all share a serious worry about cybersecurity. With the development of mobile devices and Cybercriminals now have a larger attack surface thanks to the Internet of Things (IoT), making it simpler for them to target businesses and people.

The subject of cybersecurity is full of linked discourses. Deconstructing the phrase "cybersecurity" makes it easier to place the conversation within the context of both terms Cyber and Security as well as making some of the underlying problems more obvious.

Some Significance of the research are as: -

*Confidential Information Protection:
*Continuity of business is ensured by:
*Maintenance of trust:
*Compliances:

C. The goal of the cybersecurity study is:

Some of the data's objectives are as follows:

* To recognize the cybersecurity dangers and difficulties that individuals and companies must face.

* To evaluate the performance of current cybersecurity measures and pinpoint opportunities for development.

* To research how cyberattacks affect businesses, people, and the economy.

* To assess new technological developments and their possible influence on cybersecurity.

* To suggest methods and best practices for enhancing individual and corporate cybersecurity.

II. INTRODUCTION

A. Cybersecurity Definition

The term "Cybersecurity" refers to the protection of computer systems, networks, and data from being compromised or accessed unlawfully, in order to prevent damage or loss. The implementation of various technologies, procedures, and practices is used to ensure the safety of digital information and to deter cyberattacks. [10]

A set of processes, systems, and structures are employed to protect computer networks and other electronic devices from instances where ownership rights are infringed upon. [2]

The following are current issues in cybersecurity:

Ransomware attacks: - Files encrypted by ransomware attacks are demanded to be decrypted in return for money. These attacks are increasing day by day and this can be extremely damaging to both persons and corporations.

Internet of Things (IoT) security: The IoT is a network of hardware, including computers, mobile phones, and appliances, that is linked to the Internet. The risk of cyberattacks increases along with the quantity of IoT devices. These gadgets frequently have poor security, which leaves them open to hackers.

Cloud security: Increasingly businesses are moving their data and their software to the cloud. Data breaches can greatly affect businesses and their clients; thus, cloud security is a crucial worry.

Cyber crimes

Cybercrime is the newest and maybe most difficult problem facing the online community. "Any illegal conduct that makes use of computer devices whether an instrument, target or as a means of committing additional crimes" is the definition of cybercrime." [3]

Let’s have a view of cyber-attacks in different regions all over the world.

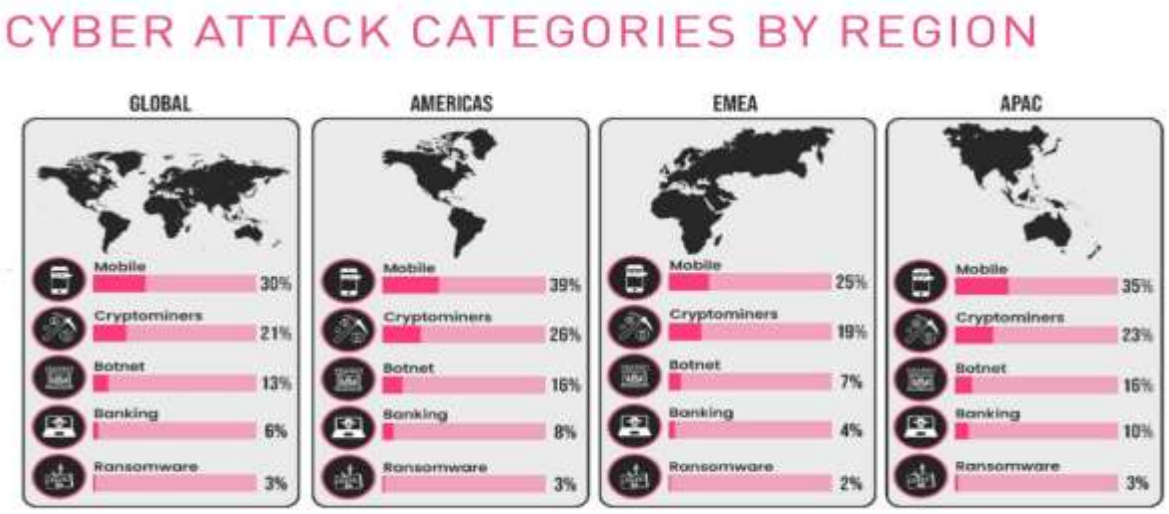

Fig 1.1(Cyberattacks categories by region [4]**)**

Prevention

Prevention is always better than cure. It is always advisable to take caution when using the internet such as.

- To protect yourself from virus attacks, always use the most recent and updated antivirus software.
- Using firewalls may be advantageous.
- To prevent fraud, never send your credit card information to an unsecured website.
- The Mumbai Police Cyber Crime Cell's technical advisor and network security consultant Shailesh Kumar Zaskar promotes the 5Ps of online security: Precaution, Prevention, Protection, Preservation, and Perseverance. [3]

  These are some of the preventions to keep us secure from Cyber-attack over the internet.

The below table describes some of the incidents/ cyber threats till 2023.

Cybersecurity threats	Date	Incident
SolarWinds Hack	Dec 2021	Hackers gained access to SolarWinds' IT management software, allowing them to conduct espionage on multiple US government agencies and other organizations.
Facebook Data Breach	Apr 2021	Personal data of over 500 million Facebook users was leaked online, including names, phone numbers, and other information.
Apple Zero-Day Exploit	Sep 2021	Hackers exploited a vulnerability in Apple's iMessage to install spyware on iPhones, affecting journalists, activists, and other targets.
Microsoft Exchange Server Hacks	Jan-Mar 2021	State-sponsored hackers exploited vulnerabilities in Microsoft Exchange Server to conduct espionage and steal data from businesses and organizations.
Inside Slack's GitHub Account Hack	December 29, 2022	Slack, one of the most popular business communication tools has become victim to a hacker.
Microsoft Azure Services Vulnerable To SSRF	On January 17, 2023	Microsoft Azure services were vulnerable to server-side request forgery (SSRF) attacks due to four vulnerabilities.

Table 1.1(incidents/ cyber threats till 2023)

Cybersecurity risks are a serious worry for businesses and individuals all around the world.

The threat environment is always changing, with new threats and attack methods appearing on a regular basis.

Annual threat numbers are essential for better understanding the nature and effect of cybersecurity threats. These data give significant insights into the most prevalent forms of attacks,

the businesses and countries most impacted, and the expenses involved with cybercrime.

In this research paper, we will review the yearly threat data since 2022 in this research report, highlighting the most relevant trends and insights. We will also discuss the consequences of these figures for businesses and people, as well as tips for strengthening cybersecurity defenses.

Annual threat intelligence statistics till 2022.

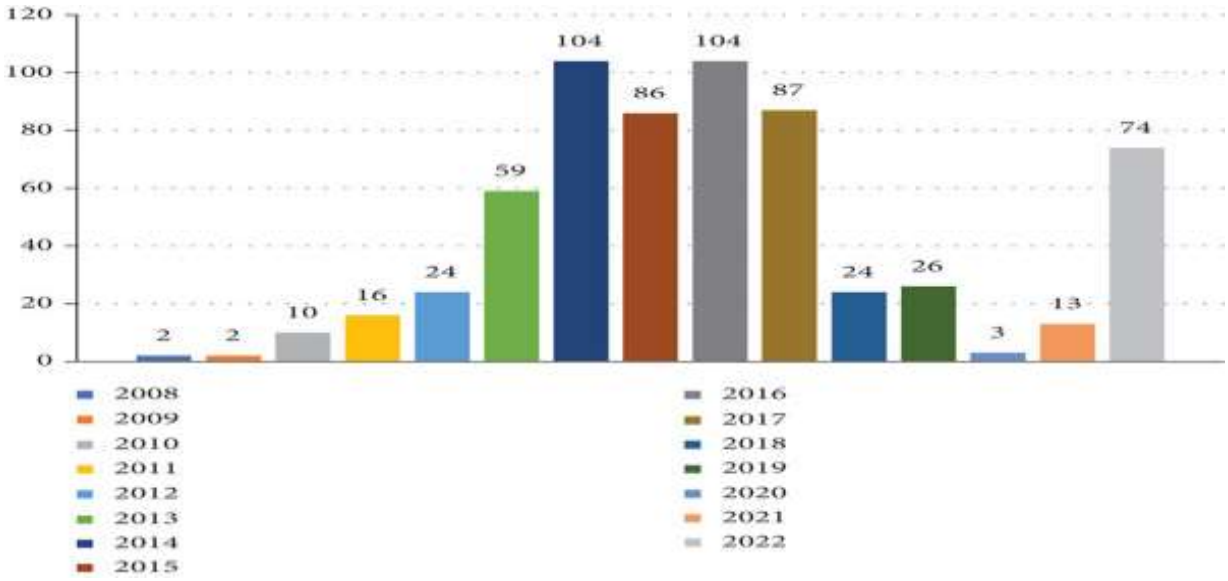

Fig 1.2 (**Threat intelligence statistics** [5])

B. Overview of Cybersecurity:

Cybersecurity is the activity of preventing unauthorized access to, theft, or damage to electronic equipment, networks, and data. As we become more dependent on technology in our daily lives, cybersecurity has emerged as a crucial concern for all parties—people, businesses, and governments.

Viruses, malware, phishing schemes, ransomware, and dos attacks are some examples of cyber threats existing nowadays. By interfering with business processes, stealing confidential information, and harming reputations, these dangers can seriously harm enterprises.[11]

Organizations adopt a variety of cybersecurity solutions, such as firewalls,

IDS, encryption, and routine security audits, to guard against these risks.

Cybersecurity is a rapidly evolving field, with cybercriminals constantly developing new methods to exploit weaknesses within networks and computers. it is critical for

individuals and organizations to stay current on the latest cybersecurity trends and best practices

in order to protect themselves from potential threats.

C. Techniques of Cybersecurity:

Nowadays, numerous cybersecurity techniques are used to secure computers, networks, and crucial information from cyber threats. Among the most commonly used techniques are:

Encryption is the process of converting data into a code or cipher that only authorized parties can read. This method is frequently used to safeguard sensitive information.

Firewalls: A firewall is a security device that monitors and regulates network traffic that is both in and out. Firewalls can be hardware or software-based. It is able to block unauthorized access and stop malware from propagating.

Authentication of data: - The papers we acquire must always be validated before downloading, which means they must be reviewed to confirm that they have not been altered and have originated from a reliable source. Typically, antivirus programs installed on the devices authenticate these documents. To protect the gadgets from infections, a dependable anti-virus program is required.

Two-factor authentication provides far more protection than the conventional username/ password combination. something you've got and something you are aware of is the two parts that constitute two-factor authentication.

With this authentication method, a person must successfully complete two authentication steps in order to gain access to a website or account. [7]

In single-factor authentication, the "something you know" element was the password. The additional element, or "something you have," is the most important part. There are various options for the component you have, including tokens, smart cards, pins/tans, and biometrics. [7]

IDS AND IPS: These systems keep track of network traffic and look for unusual behavior. It can also be used to guard against attacks by preventing traffic from known harmful sources from entering the network.

Vulnerability scanning is the process of determining weaknesses or vulnerabilities in a system or network. This can be accomplished by automated tools or manual testing, and it can aid in the identification of potential points of attack.

Malware detection and removal tools are used to detect and remove malicious software from a computer system. This includes viruses, Trojan horses, and other forms of malware.

Data backup and recovery: Data backup and recovery are critical for ensuring data integrity.

D. Purpose of the report

A cybersecurity report's purpose is to provide an overview of the organization's cybersecurity posture and to identify potential vulnerabilities, threats, and risks that could jeopardize the security of its systems and data.

The report's goal is to provide stakeholders like senior management, IT staff, and other decision-makers with an understanding of the organization's current cybersecurity state and recommendations for improving its security posture.

A summary of the organization's current security posture, a description of the potential risks and threats facing the organization, an analysis of the organization's existing security controls and their effectiveness, and a set of recommendations for improving the organization's security posture is typically included in the report.

Finally, the goal of a cybersecurity report is to provide actionable information. Insights that will assist the organization in reducing the risk of cybersecurity incidents and protecting its systems and data from unauthorized access, use, disclosure, modification, or destructive overview of the study of cybersecurity threats.

Cybersecurity is the practice of preventing unauthorized access, theft, damage, or destruction of computer systems, networks, and

digital information. It is an important field in today's interconnected world, where cyber threats are becoming more sophisticated and common.

As technology evolves at an incredible rate, so are the threats we confront in cyberspace. Every year, new threats arise, and fraudsters discover new methods to exploit flaws in our systems and networks.

Some of these challenges and threats include:

Insider Threats - Insiders who have authority over sensitive data can be a major cybersecurity concern. Organizations must have policies and procedures in place to protect themselves from insider threats.

APTs are highly focused and sophisticated attacks that are hard to detect and prevent because they may evade typical security measures.[11]

Man-in-the-middle (MitM) attacks: - MITM attacks happen whenever an attacker monitors conversations between two parties in order to eavesdrop, steal data, or mimic one of them. [13]

Supply Chain Attacks - Supply chain attacks involve gaining unauthorized access to systems and data by exploiting vulnerabilities in the supply chain.

Phishing: It is the practice of using emails to transmit malicious messages or social engineering. The purpose is to steal private data like debit card numbers and usernames and passwords from the victim. This assault is typically employed as part of a wider operation to establish a stronghold among government or company networks as an advance and persistent threat.

SQL injection (SQLI): - It tries to modify the back-end access to database information that was never meant to be displayed. SQL injections might be performed by simply typing harmful code into a susceptible website search field.[14]

Lack of Skilled Professionals - Because of the shortage of competent cybersecurity specialists, it is challenging for organizations to identify and employ the expertise needed to defend their networks and systems.

DDoS attacks: - DDoS attacks refer to a particular form of attack in which several compromised systems work together to target a single victim, ultimately resulting in the denial of service for users attempting to access the targeted system.

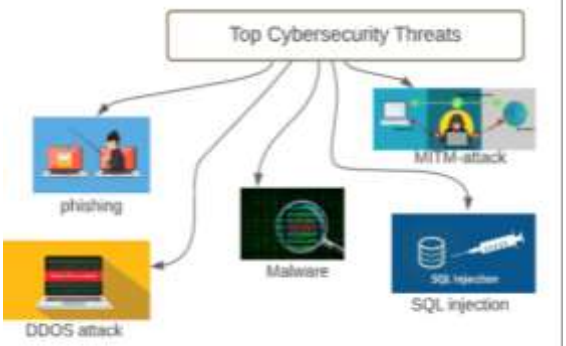

Fig1.4(Top Cybersecurity Threats)

To avoid these threats, cybersecurity experts must always be watchful and adapt their techniques to the changing situation. This necessitates requiring awareness of developing trends and prospective cybersecurity risks.

In this research paper, we will investigate the developing cybersecurity trends that are expected to shape the sector in the next years. Organizations may design more effective cybersecurity plans to secure their assets and reduce the risk of a cyberattack by spotting these trends and understanding their consequences.

Some of the upcoming cybersecurity trends include:

Artificial Intelligence and Machine Learning - AI and machine learning can help cybersecurity professionals identify patterns in cyber-attacks, allowing them to predict and prevent attacks.

Cloud Security - Because cloud computing has become an essential component of modern business operations, it has become an appealing target for cybercriminals. As a result, cloud security will become more important.[9]

Quantum computing: - use of this could result in the ability to compromise numerous encryption techniques that are presently employed to safeguard data. which could have serious implications for cybersecurity. As quantum computing becomes more widely available, new approaches to encryption will be required to ensure data security.

Zero trust security: - this cybersecurity strategy in question assumes that any network traffic could be harmful, and therefore requires that all users and devices be authenticated and verified before they are allowed to access resources. This approach can be helpful in preventing cyber-attacks, including data breaches.[9]

However, along with these trends, there are also various challenges and threats that cybersecurity professionals need to address.

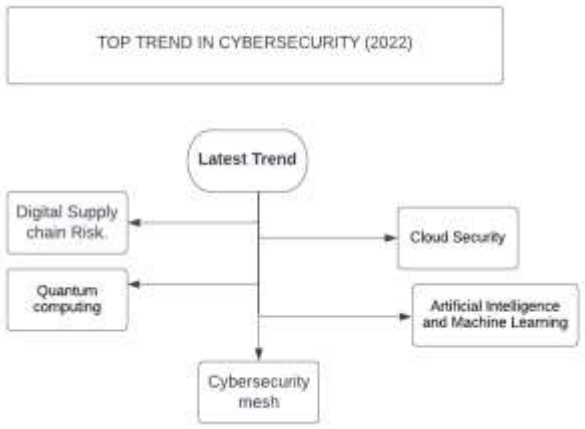

Fig1.3(trends in cybersecurity 2022)

As technology evolves continuously, cybersecurity experts must stay current on the newest trends and dangers. Continuous training and education, as well as engagement with other cybersecurity specialists and organizations, are required. Furthermore, regulatory frameworks are growing more complicated, Organizations are facing compliance challenges due to regulations related to data privacy and security, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

One of the key challenges is the lack of cybersecurity experts is a significant issue that is projected to persist in the upcoming years. Organizations must search for cutting-edge solutions to this problem, such as automation and outsourcing to bolster their cybersecurity teams.

III. METHODOLOGY

The following steps are typically included in the methodology for addressing cybersecurity challenges and threats:

The research highlights investigations made in the area of cybersecurity threats, trends, and challenges. We searched several databases using terms like cybersecurity and challenges related to it [8].

Risk assessment: - Perform a comprehensive evaluation of the risks to detect possible weaknesses and dangers in the infrastructure, data, and systems of the organization. This can involve recognizing potential hazards, examining their probability, and determining their effect on the organization.

Identification: The first stage is to identify your organization's cybersecurity concerns, trends, and threats. This can be accomplished through the evaluation of threat intelligence reports, the analysis of attack trends, and the conduct of risk assessments.

Create a Security Strategy: Based on the risk assessment results, create a comprehensive security strategy that includes a mix of hardware and software solutions, policies and procedures, and employee training and education.

Implementation entails putting in place the security strategy, which includes hardware and software solutions, policies and procedures, and employee training and education. This includes the installation of firewalls, antivirus software, intrusion detection systems, and other security measures.

Ongoing Monitoring and Evaluation: Conduct ongoing monitoring and evaluation. Monitoring and evaluation are performed to

ensure that the security strategy is effective and up to date. Regular vulnerability assessments, penetration testing, and incident response planning can all be part of this.

Continuous Improvement: Improve the security strategy on an ongoing basis by incorporating feedback from ongoing monitoring and assessment and adapting to changes in the threat landscape.

IV. LITERATURE REVIEW.

In our review of the literature, we examined numerous academic fields, such as computer science, engineering, political studies, psychology, security studies, management, education, and sociology. Our findings indicated that the most prevalent fields in our review were engineering, technology, computer science, security, and defense. Nonetheless, we also found limited instances of cybersecurity being discussed in journals related to policy development, law, healthcare, public administration, accounting, management, sociology, psychology, and education. A few of the literature reviews we encountered regarding cybersecurity are as follows:

Skilled Cybersecurity Professionals: The dearth of proficient cybersecurity experts is a major issue that is likely to persist in the upcoming years. As per a report released by (ISC)², the scarcity of qualified cybersecurity professionals around the world is projected to surge to 1.8 million by the year 2022.[15]

The Complexity of Modern Cybersecurity Systems: The complexity of modern cybersecurity systems is a significant challenge for organizations, as they require a range of hardware and software solutions to protect against a variety of threats. This complexity can make it difficult for organizations to implement and maintain effective cybersecurity strategies.

Rapidly Evolving Nature of Cyber Threats: Organizations find it challenging to keep up with the ever-evolving cyber threats. The average cost of a data breach, as per a Penamon Institute report, is $3.86 million, which escalates for organizations that encounter breaches due to new or emerging threats.

Ransomware attack: - Cyberattacks involving ransomware are on the rise, and entities of all sizes are vulnerable to such attacks. According to Cybersecurity Ventures, the global cost of ransomware damage is expected to reach $20 billion by 2021.

After conducting a literature review on cybersecurity in different fields, we have selected certain cybersecurity definitions that we believe offer comprehensive perspectives on the subject.

V. CONCLUSION

As the world becomes more interconnected, networks are being used to carry out critical transactions, making computer security an increasingly important and broad topic.

Cybercrime is constantly evolving, with new technologies and threats emerging every day, straining organizations' infrastructure security efforts. To reduce cybercrime, a proactive approach to cybersecurity is recommended, including implementing strong security measures such as firewalls, antivirus software, and intrusion detection systems. It is also important to educate staff members about cyber threats and train them to spot and report any suspicious activity.

The use of cloud computing and the Internet of Things (IoT) has introduced new challenges for cybersecurity due to their complexity, lack of standardization, and lack of regulation. While cybercrimes cannot be eliminated, efforts should be made to reduce them to ensure a safe and secure future in cyberspace.[16]

In conclusion, cybersecurity challenges, ongoing threats, and new trends continue to evolve, requiring organizations to stay vigilant and adapt their security strategies accordingly.

Studying cybersecurity threats, trends, and challenges highlights how crucial it is to approach cybersecurity in a proactive manner. Organizations must constantly evaluate their

security posture, pinpoint vulnerabilities, and put precautionary measures in place. They are able to better defend their systems, data, and reputation from the constantly changing threat environment by doing this.

The overall study concludes that cybersecurity is a dynamic, complex field that needs ongoing care and funding. Organizations can reduce their risk and protect their assets from cyber threats by following best practices, staying informed about emerging threats and trends and investing in effective security solutions.

VI. REFERENCES

[1] S. Das, "Adequacy and Limitations of the Information Technology Act in Addressing Cyber-Security Issues of Indian Power Systems," *IEEE International Conference on Power Systems (ICPS)*, 2021.

[2] D. Craigen, "Defining Cybersecurity," *Technology Innovation Management Review*, 2014.

[3] K. Dashora, "Cyber Crime in the Society: Problems and," *Journal of Alternative Perspectives in the Social Sciences*, 2011.

[4] G. &. Kantaria, " Cyber Threats and Attack Vectors during COVID-19.," *International Journal for Research in Applied Science and Engineering Technology*, no. ijraset.2020.32013., 2020.

[5] S. &. Chen, " An Automatic Assessment Method of Cyber Threat Intelligence Combined with ATT&CK Matrix," *Wireless Communications and Mobile Computing*, 2022.

[6] N. R. &. R. U. Gade, "A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies.," *research-gate*, 2014.

[7] M. M. Mogal*1, "HOW TWO FACTOR AUTHENTICATION HELPS IN CYBERSECURITY," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 06, 2022.

[8] R. N. A. A, "The Importance of Cybersecurity Education in School," *International Journal of Information and Education Technology*, 2020.

[9] A Sophos Article 04. 12v1.dNA, eight trends changing network security by James Lynne.

[10] Charles Leslie Stevenson (1908–1979) Analytic philosophe (Defining cybersecurity)

[11] Hussain, A., Mohamed, A. and Razali, S., 2020, March. A review on cybersecurity: Challenges & emerging threats. In *Proceedings of the 3rd International Conference on Networking, Information Systems & Security* (pp. 1-7).

[12] Luh, F., & Yen, Y. (2020). Cybersecurity in science and medicine: Threats and challenges. *Trends in biotechnology*, *38*(8), 825-828.

[13] Sajal, Sayeed Z., Israt Jahan, and Kendall E. Nygard. "A Survey on Cyber Security Threats and Challenges in Modern Society." *2019 IEEE international conference on electro information technology (EIT)*. IEEE, 2019.

[14] G. Tsochev, R. Trifonov, O. Nakov, S. Manolov and G. Pavlova, "Cyber security: Threats and Challenges," *2020 International Conference Automatics and Informatics (ICAI)*, Varna, Bulgaria, 2020, pp. 1-6, doi: 10.1109/ICAI50593.2020.9311369.

[15] R. A. Nafea and M. Amin Almaiah, "Cyber Security Threats in Cloud: Literature Review," *2021 International Conference on Information Technology (ICIT)*, Amman,

Jordan, 2021, pp. 779-786, doi: 10.1109/ICIT52682.2021.9491638.
[16] Pandey, A. B., Tripathi, A., & Vashist, P. C. (2022). A survey of cyber security trends, emerging technologies and threats. *Cyber Security in Intelligent Computing and Communications*, 19-33.