International Journal of Scientific Research and Management (IJSRM)
||Volume||13||Issue||12||Pages||2698-2706||2025||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v13i12.ec03

An Analysis of the Challenges in Cyber Security and the Emerging Trends in the Current Technologies

Alanoud Amer Saleem Alrkeebat

Abstract
Cybersecurity plays a significant role within the discipline of IT. Nowadays, the biggest challenge is protecting information. Whenever we think about cyber security, the initial thought that comes to mind is "cybercrimes," which are becoming more and more common every day. Companies and governments are taking many steps to prevent these cybercrimes, but despite these efforts, many individuals are still very concerned about cyber security. This paper mainly concentrates on the challenges that cyber security faces in the context of the newest technologies. It also concentrates on the most current undertakings in cyber security techniques, ethics, and trends that are transforming the profession.

Key words: cyber crime, cyber security, social media, cyber ethics, android apps, cloud computing.

Introduction

The high rate of digitalization of world economies and the unprecedented rate of technological implementation have radically changed the situation with cybersecurity (Bailey et al. 2022; Ibrahim 2022). As cybercrime costs are anticipated to hit 10.5 trillion per year by 2025, the largest economic wealth transfer in history, awareness and the need to tackle cybersecurity issues become not only a technical requirement, but a life-or-death need to the global economy (Dastagiraiah, 2025).

The growth of Internet of Things (IoT) devices, artificial intelligence, and cloud-based infrastructure has increasingly widened the scope of attack that cybercriminals can carry out at an enormous scale, as it has brought more vulnerabilities that protection system frameworks were not made to handle (Dhayanidhi, 2022). Modern cyber threats have now turned into more complex multi-vector attacks by taking advantage of advanced persistent threats (APTs), zero-days exploits, and social engineering tricks to steal critical infrastructure, personal information, and organizational resources (Kayode et al. 2025). This change requires a holistic investigation of the technical and human aspects that lead to cybersecurity weaknesses and the evaluation of how new technologies like machine learning, quantum computers, and blockchain can be used to improve defensive capabilities, and at the same time create new security issues.

Research Problem Statement

Although research on cyber security in specific areas has been carried out extensively, there is still a pressing gap in full investigation of how the new technologies are working together to redefine the threat and take a toll on the current security strategies. This research paper fulfills this gap by looking at the intersection of several technological trends and how they jointly affect cybersecurity practices.

Research Questions

1. What is the overall effect of new technologies on the cybersecurity threat?
2. Which security pitfalls are posed by the convergence of several new technologies that are the most alarming?

Cyber Crime

According to Goni et al., (2022) any unlawful conduct that mainly entails the usage of a computer device for stealing and commission is described as cybercrime. Therefore, the cybercrime context is broadened by the

Jordan Ministry of Justice to encompass behaviors that are unlawful and stores evidence on a computer (Al-Sarayreh, D. R. (2024). In addition to crimes which have been made possible by computers, like network attacks and the spread of computer malware, the expanding list of cybercrimes also includes computer-based variants of pre-existing crimes, like identity fraud, stalking, harassment, and terrorism, have grown to be important issues for both people and nations. Broadly, cybercrime refers to any crime where an individual utilizes a computer and the internet to steal identity, sell illegal goods, stalk the victim or disrupt business operations using malicious software (Deora & Chudasama, 2021). With technology continually assuming an important role in the lives of people, cybercrimes are also going to increase in the same measure.

Cyber Security

Nikiforova, (2022) indicated that data security and privacy has remained the highest priorities of all firms in the field of security. We live in the world where all data are stored digitally or cyber-wise. Users are also able to communicate with family members and close friends in a safe space within the social networking sites. The cybercriminals will continue to target social media sites as a means of accessing personal data of the home users (Kaur et al., 2024). Besides social networking, it is also necessary to observe all the security measures whenever carrying out financial transactions.

Jordan as a country exhibits the changing face of the digital threat situation and the subsequent improvement of defence methodologies. As the initial quarter of the year 2025 report of the National Cyber Security Centre (NCSC), the publication provides many details about the cybersecurity level of the country and its response to incident and cyberattacks, which may be considered groundbreaking (Sharif & Mohammed, 2022).

At the beginning of 2025, Jordan NCSC received 1,369 cybersecurity incident situations within the framework of two-stage precarious kinds of triage (Sharif & Mohammed, 2022). This systematic method made it easy to categorize and rank threats according to its severity in affecting the national infrastructure and the security of a country. These were especially 77 events that needed expert intervention because they had the sense of national importance. As much as this is a significant reduction in half that of the 100 high-priority incidents that were reported in Q4 2024, it nonetheless portrays a consistent and challenging sophisticated cyberattacks facing Jordan system and infrastructure assets. Most of the reports 1,292 incidents were observed to be handled in the standard general triage process of NCSC. This figure denotes a meager 2.7% increase against the 1,258 reports dealt with during the last quarter. Yet, in the perspective of historical record during the last eight quarters, this figure is lower than the established average and this indicates better preventive effort, or possible underreport. The information is presented in the following figures and tables;

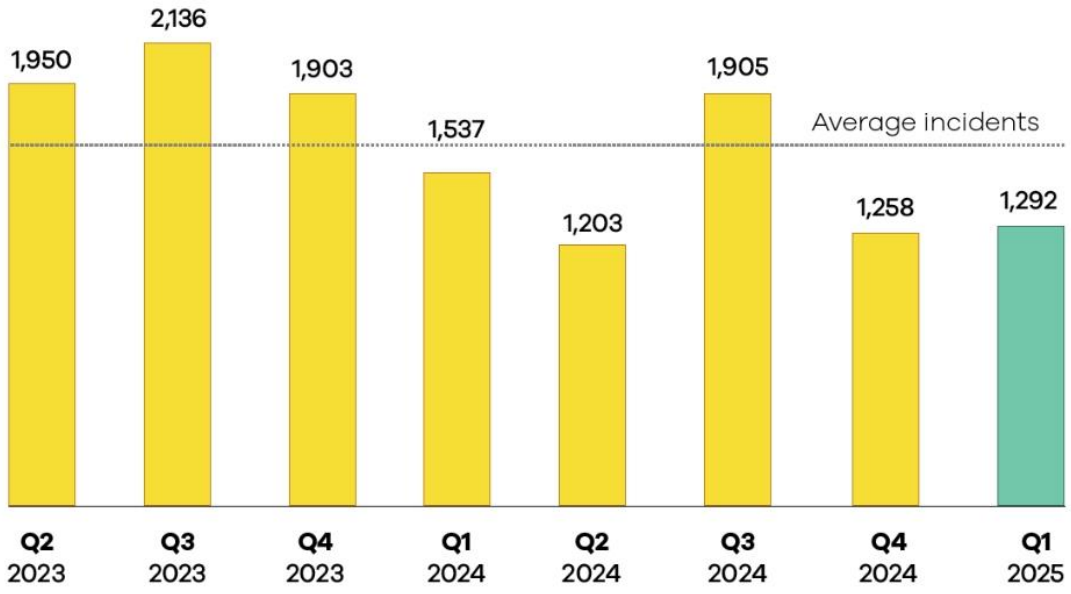


Figure 1

YEAR	QUARTER	INCIDENTS
2025	1	1,292
2024	4	1,258
2024	3	1,905
2024	2	1,203
2024	1	1,537
2023	4	1,903
2023	3	2,136
2023	2	1,950

Table 1

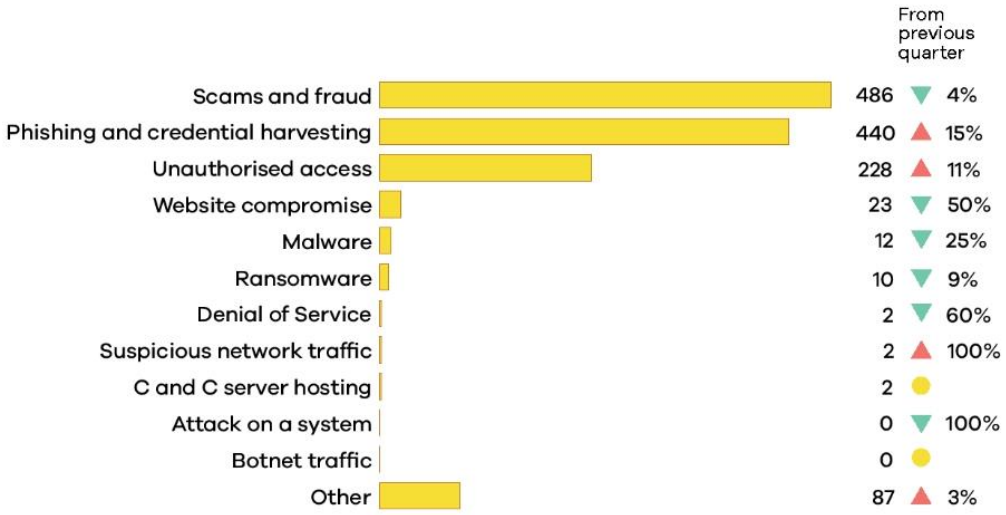


Figure 2

INCIDENT CATEGORY	INCIDENT COUNT	CHANGE FROM PREVIOUS QUARTER
Scams and fraud	486	-4%
Phishing and credential harvesting	440	15%
Unauthorised access	228	11%
Website compromise	23	-50%
Malware	12	-25%
Ransomware	10	-9%
Denial of Service	2	-60%
Suspicious network traffic	2	100%
C and C server hosting	2	N/A
Attack on a system	0	-100%
Botnet traffic	0	N/A
Other	87	3%

Table 2

The new threats that affect Android are of a higher sophistication, where the Trojan banker attacks are rising by 196 percent by 2024 and the figures of smartphone attacks that were observed in the world exceed 33.3 million (Ali et al., 2024). As compared to earlier broad-spectrum malware, modern-day threats seem to be targeting high-value assets such as banking credentials and wallets of cryptocurrencies across Android smartphones, tablets, and smart television sets. iOS is no longer safe, with significant Apple malware surfacing in 2024, affecting Mac to iPhone devices, as the walled garden paradigm software has been effectively penetrated by advanced threat actors (Hodson, 2024). MacOS malware have increased exponentially, with almost twenty malware families recorded in 2024, which included stealers, backdoors and ransom Cross-platform development platforms such as React Native and Flutter open up the potential of cybercriminals to develop unified malware which affect multiple operating systems simultaneously, and with AI-based threats learning on the fly, detection techniques are becoming ineffective across all platforms.

Trends Changing Cyber Security

The following are some of the trends that are contributing greatly to cyber security.

Cloud computing along with its services

Over the past few years, all types of business are slowly migrating to cloud services. In other words, the planet becomes more and more important closer to the clouds (Golightly et al., 2022). Since messages can evade the traditional entry points of control, this latest trend can be a major threat to cyber security. Moreover, policy limits on web applications and cloud services will also have to alter to ensure the protection of important data should it be lost, and the number of programs existing in the cloud is growing (Abdulsalam and Hedabou, 2021). Since cloud services are developing their own models, numerous security issues are being questioned. Despite the numerous advantages that the cloud can offer, it must always be remembered that the security issues will keep increasing with the expansion of the cloud.

Web servers

Web applications continue to be susceptible to attacks that intend to send malicious code or collect information. Hacked legal web servers are used by cybercriminals to distribute their malicious programs (Choi et al., 2023). However, data stealing hacks are also quite a threat and much of them are covered by the media. Web server and online application protection should now be given more serious consideration. In particular, web servers can offer the best platform with which cybercriminals can access data. Thus, Whittaker et al (2023) explained that to avoid being a target of such crimes, one must always operate a safer browser, especially when performing significant transactions.

APT's and targeted attacks

APT (advanced persistent threat) is an entirely new type of malware used in cybercrime. Network security solutions such as intrusion prevention systems (IPS), web filtering and so on have played an important role of identifying such type of targeted attacks (typically after its initial intrusion) over the decades (Gupta et al., 2023). Network protection must interact with additional safety measures to identify assaults as attackers get more bolder and employ more nebulous tactics. To avoid further dangers in the future, we must thus enhance our security methods.

IPv6: New internet protocol

The new IPv6 protocol is replacing the old IPv4 protocol which formed the basis of our networks and the Internet as a whole. It does not simply involve transfer of IPv4 facilities to secure IPv6. Despite the fact that IPv6 is a full replacement as far as the number of IP addresses available grows (Piraux et al., 2022), some rather basic changes to the protocol should be considered in the security policies. In order to reduce the risks of cybercrime, it is therefore always better to move to IPv6 as soon as possible.

Mobile Networks

Now we are able to communicate with any individual within any location in the world. Security is however a big concern of these mobile networks. Today firewalls and other security measures are becoming increasingly susceptible as an increasing population deploys devices such as tablets, PCs, and mobile devices among other gadgets that require supplementary security measures over and above those of the apps they use (Nidup, 2021). The security concerns of these mobile networks have to be in our mind at all times. Also, since mobile networks are highly susceptible to these cybercrimes, much care should be taken with regard to their protection.

Encryption of the code

Encryption is the practice of securing communications or information by encrypting it to prevent its ability to be read by hackers or listening devices (Hazra et al., 2024). An encryption strategy encrypts the message or data with an encryption algorithm to turn it into an incomprehensible ciphertext. This is normally done using an encryption key which states the way the message should be encoded. Encryption ensures the safety of data integrity and privacy. This, however, poses more cyber security challenges with increased use of encryption (Oladoyonbo et al., 2024). Data in transit, such as that being sent over networks (such the e-commerce or Internet, wireless microphones, mobile phones, wireless intercoms, etc., can also be protected by encryption. Therefore, one may determine whether there is any information leaking by encrypting the code.

As a result, some themes that are transforming cyber security globally are listed above. The following lists the main network dangers.

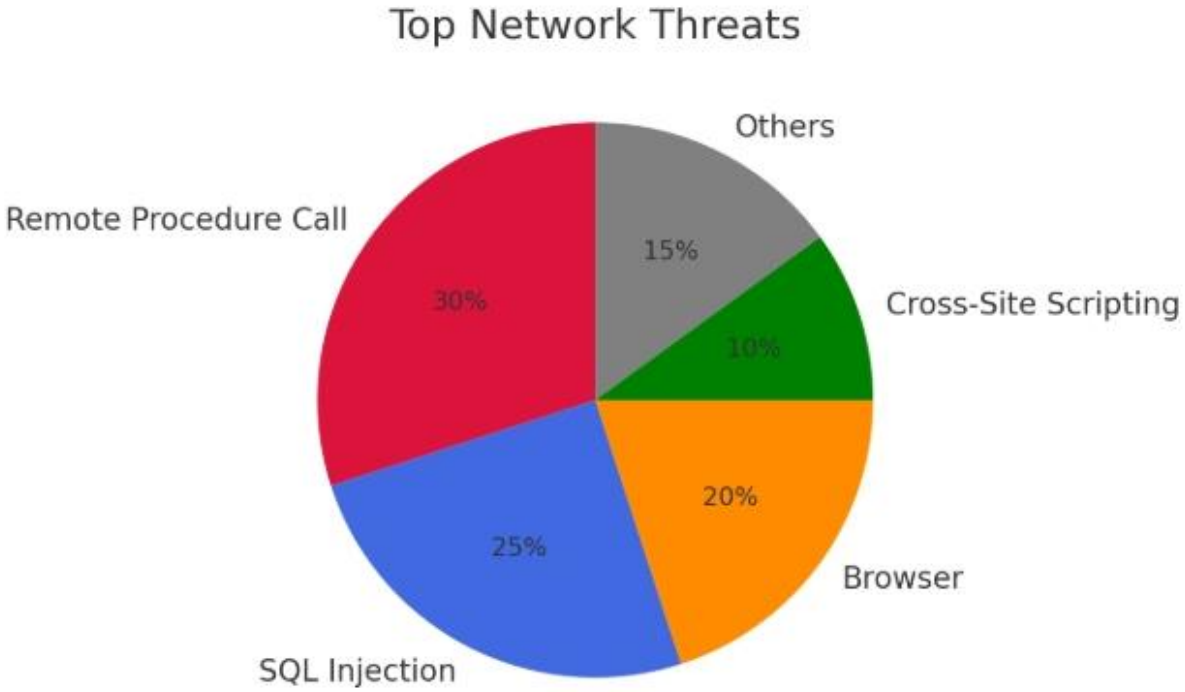


Figure 3

The main risks to networks and cyber security are depicted in the pie chart above.

Role Of Social Media in Cyber Security

The world is becoming more connected and social, and businesses should be able to think of original approaches to protect personal data. The social media is one of the leading contributors to personal cyber threats and also a large factor in cyber security (jalal yousef Zaidieh, 2024). The risk of an assault is growing rapidly as well as social media usage by employees. Because most of them use social media or social networking sites daily, they have become a significant tool used by cybercriminals to steal valuable information and ruin personal data.

In a world where we are eager to divulge our personal information, businesses must make sure they are equally quick to recognize dangers, take immediate action, and prevent any type of breach (Hendrycks et al., 2023). Using these social media is a good lure to attract the data and information that they require because the user will be easily attracted to these social media. People must thus take the necessary precautions to avoid losing their information, particularly while using social media. The unique problem that social media poses for businesses is rooted in people's capacity to disseminate information to millions of others (Rathi et al., 2024). Social media allows everyone the ability to communicate economically sensitive information, but it also gives them the ability to spread incorrect information, which may be just as harmful. One of the new threats mentioned in the Global threats 2024 report is the quick dissemination of misleading information on social media (Tomassi et al., 2024).

Even though cybercrimes are a possibility, not all businesses can afford to stop using social media because it plays a significant role in the exposure of their brand. Rather, to prevent it before any harm is caused, they must possess alternatives that will warn them of it. However, companies ought to bear this in mind, and recognize the importance of information analysis especially in social interactions and provide appropriate security to avoid risks. An effective management of social media involves applying proper technology and some rules (Balkin 2021).

Cyber Security Approaches

Password security and access control

A basic method of safeguarding our data has been the application of a password and user name. In terms of cyber security, this can be among the initial steps.

Data authentication

Before being downloaded, the papers we receive have to be continually validated, implying that verification has to come from a trustworthy and dependable source and to be undamaged. Device anti-virus software often performs the authentication of these documents. Therefore, to safeguard the devices from infections, a strong anti-virus program is also necessary.

Malware scanners

This program normally scans through all the files and papers in the system to detect the dangerous viruses or malicious codes. Examples of dangerous software that are frequently lumped collectively and alluded to as malware include Trojan horses, viruses, and worms.

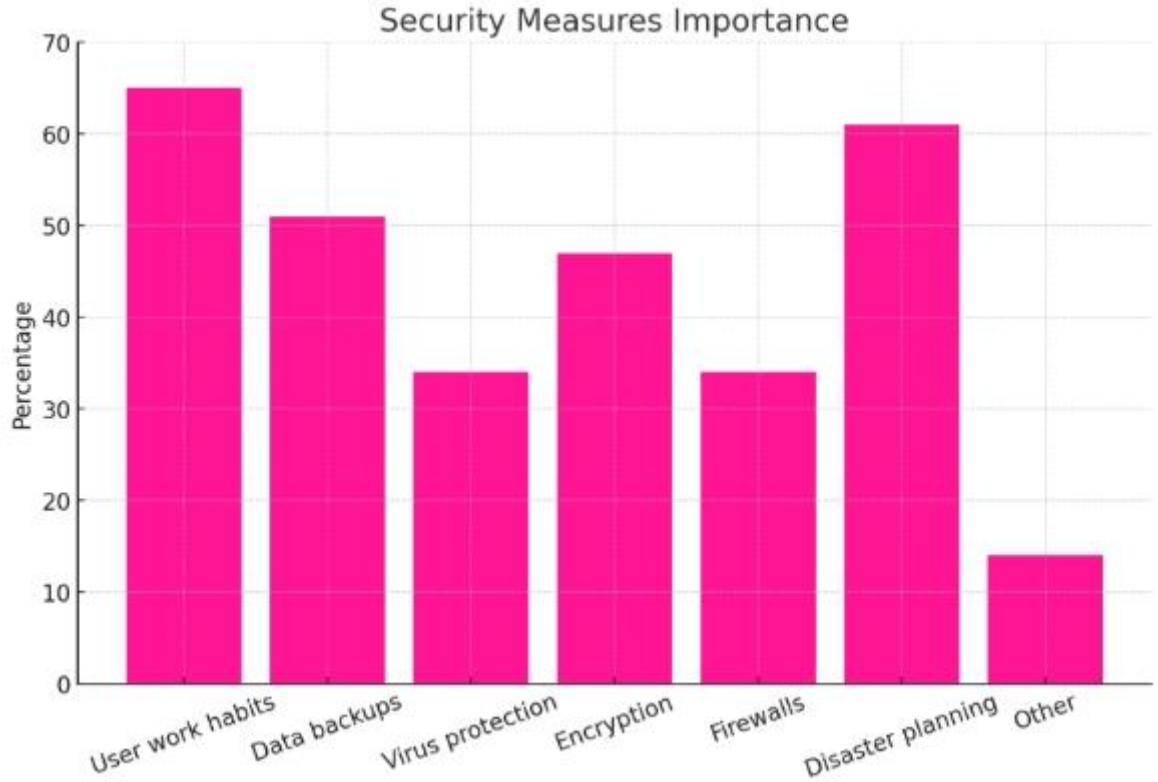
Firewalls

A firewall is a hardware or software that assists in blocking viruses, worms, and hackers who might want to gain access to your computer over the Internet (Gao et al 2021). The firewall filters every communication going in or out of the internet and examines it and blocks links that do not conform to the predefined security standards. Consequently, firewalls can play an important role in detecting malware.

Anti-virus

An antivirus software is a computer program that identifies, prevents, and responds to dangerous software, such as viruses and worms (Kondrashenko and Grechykhina, 2021). Most antivirus programs have an auto update option which enables it to acquire virus profile which it can then proceed to scan new threats as and when they are detected. Anti-virus software is one of the requirements in every system.

Table 4: Approaches on cyber security



Cyber Ethics

Cyber ethics are simply the rules that govern the internet. We have a fair chance of utilizing the internet in a responsible and secure manner when we follow these cyber principles. Here are a handful of them:

DO communicate and socialize via the Internet. Email and instant messaging make it easy to communicate with colleagues, keep in touch with friends and family and share ideas and information with people, both locally and around the world.

Do not be an on-line bully. Do not attempt to harm anyone by calling them names, lying on them, sending them embarrassing photos or doing anything else.

Also, because the internet is considered as the best library in the world and it stores the knowledge of all subjects, it is always important to use the internet properly and legally.

Never give a personal information to any party because there are high chances that someone will misuse it and expose you to trouble.
Some of the cyber ethics that an individual must follow when using the internet are mentioned above. We are taught proper rules at a young age, and this is the same case in the cyberspace.

Significance of the Study
This study adds to the body of literature on cybersecurity because it offers a comprehensive perspective on the nature of interdependent vulnerabilities that are formed by emerging technologies. Contrary to other research works that have analyzed technologies as individual constructs, this paper provides a holistic study that discloses the systemic security issues.

Practical Applications and Beneficiaries
Small and Medium Enterprises (SMEs): This paper offers available cybersecurity plans that are based on resource-limited settings that cater to the unique requirements of the organizations that cannot afford enterprise-grade cybersecurity measures.
Large Corporations: The study provides a strategic view to redesign old security technologies to meet the new threat vectors potentially leading to millions in saved breach prevention expenses.
National Security Agencies: The paper gives evidence-based findings on how national strategies and regulating frameworks on cybersecurity should be updated.
Developing Nations: There are special considerations of cybersecurity capacity building that provide developing nations with viable avenues through which they can improve digital security posture.
Cybersecurity Researchers: This text lists the areas of priority on future research and forms a basis of the creating next-generation security technologies.

Conclusion
Computer security is a general phenomenon that is gaining relevance as the world continues to become more interconnected, with networks being used to transact crucial functions. Cybercrime and information security keep taking turns every new year and in such a way that are unpredictable. In addition to the new cyber arsenals and threats that are appearing daily, new, disruptive technologies are rendering it challenging to even protect infrastructure, and enterprises require new platforms and intelligence to do so. To ensure the future of safety and security in cyberspace, we should do all in our power to reduce cybercrimes, even though there is no foolproof answer.

REFERENCES

1. Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. *Future Internet*, *14*(1), 11.
2. Al-Sarayreh, D. R. (2024). Jordanian Cybercrime Law No.(17) of 2023 between Regulating Social Media Sites and Restricting Freedom of Opinion. *Scholars International Journal of Law, Crime and Justice*, *7*(09), 339-351.
3. Bailey, D. E., Faraj, S., Hinds, P. J., Leonardi, P. M., & von Krogh, G. (2022). We are all theorists of technology now: A relational perspective on emerging technology and organizing. *Organization Science*, *33*(1), 1-18.
4. Balkin, J. M. (2021). How to regulate (and not regulate) social media. *J. Free Speech L.*, *1*, 71.
5. Choi, K. S., Lee, C. S., & Merizalde, J. (2023). Spreading viruses and malicious codes. In *Handbook on Crime and Technology* (pp. 232-250). Edward Elgar Publishing.
6. Dastagiraiah, C. (2025). Online Secure Transaction System with Crpytography.
7. Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. *Journal of communication engineering & Systems*, *11*(1), 1-6.
8. Dhayanidhi, G. (2022). Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing.
9. Golightly, L., Chang, V., Xu, Q. A., Gao, X., & Liu, B. S. (2022). Adoption of cloud computing as innovation in the organization. *International Journal of Engineering Business Management*, *14*, 18479790221093992.

10. Goni, O., Ali, M. H., Alam, M. M., & Shameem, M. A. (2022). The basic concept of cyber crime. *Journal of Technology Innovations and Energy*, *1*(2), 16-24.
11. Gupta, N., Jindal, V., & Bedi, P. (2023). A survey on intrusion detection and prevention systems. *SN Computer Science*, *4*(5), 439.
12. Hazra, R., Chatterjee, P., Singh, Y., Podder, G., & Das, T. (2024). Data encryption and secure communication protocols. In *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning* (pp. 546-570). IGI Global.
13. Hendrycks, D., Mazeika, M., & Woodside, T. (2023). An overview of catastrophic AI risks. *arXiv preprint arXiv:2306.12001*.
14. Hodson, C. J. (2024). *Cyber risk management: Prioritize threats, identify vulnerabilities and apply controls*. Kogan Page Publishers.
15. Ibrahim, H. (2022). A review on the mechanism mitigating and eliminating internet crimes using modern technologies: Mitigating internet crimes using modern technologies. *Wasit Journal of Computer and Mathematics Science*, *1*(3), 50-68.
16. jalal yousef Zaidieh, A. (2024). Combatting cybersecurity threats on social media: Network protection and data integrity strategies. *Journal of Artificial Intelligence and Computational Technology*, *1*(1).
17. Kaur, G., Bonde, U., Pise, K. L., Yewale, S., Agrawal, P., Shobhane, P., ... & Gangarde, R. (2024). Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime. *Engineering Proceedings*, *62*(1), 6.
18. Kondrashenko, I., & Grechykhina, N. (2021). Varieties of computer viruses and methods of protection against them. Antivirus programs. *НАУКА–ВИРОБНИЦТВУ*, 13.
19. Martin, A. S. (2023). Outer space, the final frontier of cyberspace: Regulating cybersecurity issues in two interwoven domains. *Astropolitics*, *21*(1), 1-22.
20. Nidup, Y. (2021). Awareness about the online security threat and ways to secure the youths. *Journal of Cybersecurity*, *3*(3), 133.
21. Nikiforova, A. (2022, April). Data security as a top priority in the digital world: preserve data value by being proactive and thinking security first. In *The International Research & Innovation Forum* (pp. 3-15). Cham: Springer International Publishing.
22. Oladoyinbo, T. O., Oladoyinbo, O. B., & Akinkunmi, A. I. (2024). The Importance Of Data Encryption Algorithm In Data Security. *Current Journal of International Organization of Scientific Research Journal of Mobile Computing & Application (IOSRJMCA)*, *11*(2), 10-16.
23. Rathi, S. K., Keswani, B., Saxena, R. K., Kapoor, S. K., Gupta, S., & Rawat, R. (Eds.). (2024). *Online social networks in business frameworks*. John Wiley & Sons.
24. Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trend. *World Journal of Advanced Research and Reviews*, *15*(1), 138-156.
25. Tomassi, A., Falegnami, A., & Romano, E. (2024). Mapping automatic social media information disorder. The role of bots and AI in spreading misleading information in society. *Plos one*, *19*(5), e0303183.
26. Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, *51*, 2172-2175.
27. Whittaker, J. M., Edwards, M., Cross, C., & Button, M. (2023). "I have only checked after the event": Consumer approaches to safe online shopping. *Victims & Offenders*, *18*(7), 1259-1281.