IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14220

Contemporary Challenges in Cyber Security: A Comprehensive Review

Amandeep Kaur

Dept. of Computer Science and Applications, DAV University, Jalandhar

Email: Amandeep.kaur@davuniversity.org

ORCID: 0000-0003-1660-2500

Abstract: In today's fast-paced digital era, businesses are rapidly transforming by embracing electronic transactions to streamline their operations. With the increasing reliance on digital platforms, companies are actively leveraging social networking apps to attract and engage with customers. This shift has given rise to a new form of commerce known as "social commerce," where social media networks facilitate buying and selling activities. However, the adoption of new technologies in various business processes introduces a plethora of security challenges. One significant concern is the rampant use of social media for product marketing, which has led to the proliferation of fake information and counterfeit product reviews. These deceptive practices can significantly influence consumer purchasing decisions, complicating the ability of business organizations to provide accurate and trustworthy marketing information. Addressing these security issues requires robust models and frameworks that can effectively safeguard against cyber threats. This paper delves into the realm of cybersecurity, examining its frameworks and strategies for protecting personal information in the digital landscape. By conducting a systematic review of existing literature, the author aim to uncover the cybersecurity challenges faced by business organizations and their customers. The study explores various prevention methods to mitigate cybercrime and ensure customer safety. Additionally, it offers valuable insights and recommendations for future research to further enhance cybersecurity measures.

Keywords: Cybersecurity Frameworks, Cyber Threats, Risk Management, Malware

I. INTRODUCTION

Technology plays a significant role in our daily lives. Technology has significantly transformed the way we conduct business [24]. It has elevated traditional commercial practices to a higher degree. Emerging technologies significantly influence the cost, quality, and operational methods of goods and services in businesses [23]. Business is the exchange of goods or services for anything of value. To be more precise, it refers to the act of exchanging commodities or services for monetary compensation [5]. The use of technology has significantly changed how companies conduct their operations. Online shopping, also known as e-business [21], refers to the use of computer technology in business transactions. E-commerce conducts transactions and activities exclusively through the Internet. A website serves as the primary platform for e-commerce, although it can also leverage additional technologies such as email. E-commerce encompasses three crucial components: the digital marketplace, online retail, and internet-based transactions. An end user can remotely purchase a good or service using an app or technology that facilitates the sale [12]. The e-commerce landscape continues to evolve with the emergence of novel technologies and their applications. Researchers from other disciplines, including business and technology, are collaborating to improve the methodology's utility and value. However, these alterations have also presented the firm with several challenges [9]. Cyber security is a prominent challenge in the realm of e-commerce, and it is both prevalent and critical.

Cybercriminals consistently target e-commerce enterprises and their clientele, subjecting them to cyberattacks. The most valuable resource in the field of e-commerce is confidential client data, which is typically the target of malicious individuals. They have the ability to extract data from online store databases and employ malicious software such as malware, ransomware, or e-skimming techniques.

In addition, they can employ distributed denial-of-service (DDoS) attacks or engage in phishing attempts to launch their attacks. Given the increasing prevalence of e-business and e-commerce, it is evident that a greater number of opportunities are on the horizon. Nevertheless, there persist unresolved issues, such as cyber security, that necessitate resolution. Cybercriminals continually enhance their technology and expertise, similar to e-commerce enterprises, in order to identify vulnerabilities in the system and exploit them. Therefore, it is critical to carefully examine technology's advantages and disadvantages and effectively address the associated issues.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14220

It is critical to acknowledge that utilizing contemporary technology to address cybersecurity issues incurs high costs that are beyond the financial means of the majority of e-commerce enterprises. Several firms refrain from conducting cybersecurity risk monitoring due to its high cost while simultaneously neglecting to consider the potential long-term advantages [13]. While investing in technology does significantly enhance security, smaller and newer firms face challenges in doing so.

This paper provides a brief overview of the security issues that are prevalent in the digital domain. The paper is structured in the following manner: The research objectives are delineated in Section II. Section III investigates the importance of implementing safeguards to safeguard against cyber hazards. Section IV analyzes and organizes substantial cybersecurity concerns. The strategies for preventing security vulnerabilities are outlined in Section V. Future research directions are provided in Section VI, while the final section concludes the investigation.

II. RESEARCH OBJECTIVES

- To investigate how the rise of social commerce has influenced cybersecurity challenges for businesses and consumers, particularly focusing on the proliferation of fake information and counterfeit product reviews.

- To examine the prevalent types of cyber threats faced by e-commerce businesses and their customers, including malware, ransomware, phishing, and DDoS attacks, and assess their impact on consumer trust and business operations.

- To conduct a systematic review of existing cybersecurity frameworks and models to determine their effectiveness in addressing the unique challenges posed by the digital landscape, especially for e-commerce and social commerce.

- To propose new or improved risk management strategies that businesses can adopt to enhance their cybersecurity posture, taking into account the evolving nature of cyber threats and technological advancements.

- To assess the effectiveness of employee training and awareness programs in reducing the likelihood of cybersecurity breaches and improving overall organizational security culture.

- To Provide insights and recommendations for future studies aimed at enhancing cybersecurity measures in e-commerce and social commerce environments.

III. THE INDISPENSABLE ROLE OF CYBERSECURITY IN PROTECTING SENSITIVE INFORMATION

The importance of cyber protection is steadily increasing. Our current society is increasingly reliant on technology, and there is little indication that this trend will reverse. Social media platforms openly disseminate confidential information, potentially leading to identity theft, for public viewing. Cloud storage services such as Dropbox and Google Drive are currently utilized for the storage of sensitive data, including Social Security details (SSNs), credit card details, and bank account information [20].

People use computers on a daily basis, whether they are individuals, small enterprises, or large global corporations. The emergence of cloud computing services, inadequate security measures for cloud-based services, the proliferation of smartphones, and the Internet of Things (IoT) have introduced numerous cyber security concerns that were absent in previous decades. Despite the increasing similarity of abilities, it is crucial to understand the difference between cyber security and computer security [2].

In the current era of rapid digitalization, cyber security has emerged as a crucial element for ensuring the protection of individuals, organizations, and nations. The pervasive use of technology in daily activities, such as banking, communication, and data storage, has resulted in a situation where vulnerabilities are widespread. Here are a few key factors that emphasize the critical importance of cyber security:

- **Safeguarding Sensitive Data**: Both organizations and individuals save large quantities of sensitive information on the internet, including personal identity details, financial records, and confidential business data. Cybersecurity protects this information from unauthorized access and future breaches, thereby preventing identity theft and financial harm.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14220

- **Ensuring the Protection of Business Activities:** Cyberattacks have the potential to interrupt business activities, resulting in substantial financial losses and reputational harm. Cybersecurity guarantees the uninterrupted functioning of enterprises, preserving consumer trust and loyalty.

- **Adherence to requirements:** Many sectors must adhere to stringent data protection requirements such as GDPR, HIPAA, and PCI DSS. Implementing cyber security measures enables firms to adhere to these requirements, thereby preventing legal ramifications and bolstering their reputation in the market.

- **Addressing the Risks of Cyber Threats:** Cyber threats, including malware, ransomware, phishing, and denial-of-service assaults, are continuously developing. An effective cyber security framework aids in the identification, evaluation, and reduction of these threats, safeguarding digital assets and network infrastructure.

- **Safeguarding Reputation and Trust:** A data breach can have enduring consequences for a company's standing. Organizations can establish trust and credibility with their clients by prioritizing cyber security and demonstrating their dedication to safeguarding customer information.

- **Promoting Innovation and Expansion:** By implementing robust cyber security measures, firms may fearlessly embrace emerging technologies like cloud computing, IoT, and AI without being concerned about the potential hazards involved. This promotes creativity and enables expansion in an ever more competitive digital environment.

- **National Security**: In order to ensure national security, cybersecurity is of utmost importance. It is imperative for governments to protect their infrastructure, population, and sensitive data from cyber assaults sponsored by other states and unscrupulous individuals. Robust cyber security measures are vital for preserving national stability and security.

Cybersecurity is crucial for preserving sensitive data, maintaining company operations, promoting innovation, and protecting national interests. With the ongoing evolution of the digital landscape, the significance of strong cyber security measures will inevitably grow, necessitating individuals and organizations to prioritize their strategies for defending against cyber threats.

IV. ESSENTIAL CHALLENGES IN CYBER SECURITY

The success of cyber security measures is contingent upon the precautions and decisions that individuals make during the installation, operation, and use of their systems [1]. Various frameworks have been developed in an effort to address the issue of evaluating cyber security. Nevertheless, the frames have encountered distinct issues, despite their initial success during the manufacturing process [22]. New technologies [10] and the scale of the facilities are among the factors that impose restrictions. Security issues are frequently perceived as a compromise between safety standards and other advantages [14, 15, 16].

• **Compliance and Regulatory Requirements:** Organizations are required to navigate the intricate and constantly changing regulatory landscapes that pertain to data protection and cyber security. Particularly for global organizations that are required to comply with multiple jurisdictions, the process of ensuring compliance with a variety of laws can be resource-intensive and difficult.

• **Integration of Emerging Technologies:** The accelerated adoption of technologies such as the Internet of Things (IoT), artificial intelligence (AI), and cloud computing has introduced new vulnerabilities. It is a substantial challenge to ensure that these technologies are securely incorporated into existing systems while simultaneously managing the associated risks.
• **Response to and Recovery from Incidents:** Despite the greatest efforts, breaches may still occur. In order to promptly contain and mitigate the consequences of a compromise, organizations must establish effective incident response plans. Minimizing damage necessitates the development and testing of these plans, as well as strategies for business continuity and disaster recovery.

• **Professionals in the field of cybersecurity:** The National Institute of Standards and Technology (NIST) is endeavouring to foster collaboration among various agencies regarding the National Initiative for Cybersecurity Education (NICE). The agency's primary objectives are to promote awareness, education, training, and professional development in the field of cyber security. They developed the Cybersecurity Workforce Framework. From this framework, it is evident that recognition is an integral component of the educational process. also ensures the security of

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14220

computer infrastructure, as the term is used in this context. Additionally, the framework fails to account for the rapid development of new technologies, which complicates the management of cyber security risks [6]. It is also recommended by scholars that cybersecurity standards and procedures be reviewed frequently and that they be adequate [22]. The experts also assert that the frameworks do not address hazards that exploit vulnerable individuals; therefore, it is necessary to develop risk management strategies [3]. Additionally, the authors assert that there are insufficient laws in place to address cybercriminals. Finally, a successful security strategy may incorporate the modelling of business processes [26].

• **Security measures to safeguard confidential information stored on computers:** Cybersafe is a term that has been employed to denote a collection of activities, procedures, and measurements that are designed to safeguard your personal information and computer from potential hazards [11, 19]. PPM 310-22, the Cyber-Safety Program policy of any business, mandates that all devices connected to the company's digital communication network must adhere to specific security standards. The majority of departments submit annual reports that demonstrate their compliance with the regulations, as mandated by the system. Additionally, there are numerous services that have been established to assist all instructors, staff, and students in adhering to cyber safety standards. These services are described in detail. Online safety can be jeopardized by viruses, hackers, identity criminals, and spyware [7]. The computer is infected with the virus through the exchange of files or the inclusion of an attachment in an email. An assault on a single computer can cause issues with all of the computer networks. Hackers are individuals who remotely access a computer. These individuals employ computers to transmit spam, viruses, and other items that disrupt the functionality of other individuals' computers. Those who access your personal information, such as your social security number or bank account number, without your consent are known as identifying criminals [27]. When you download other programs, spyware is installed on your computer. It monitors your online activities and transmits personal information to others without your consent. A company that neglects to address the security of personal information and users' computers may encounter a variety of additional issues in addition to those previously discussed. Consequences may include the loss of access to the campus computer system, private information, collaboration and access to useful university information, research on specific digital information cases, a decrease in public trust and offer opportunities, pursuit, internal conflict action, and/or termination of employment.

• **Research on the services offered by firewalls:** The efficacy of personal firewall systems was examined by Al-Fayyad et al. [4] through the establishment of a planned tour to determine which components of the design could potentially violate usage rules. Four current firewalls were employed in the investigation of the effectiveness of personal firewalls on Windows XP: Norton 360 V. 2.0.0.242, Trend Micro Internet Security V. 16.00.1412, Zone Alarm V. 7.1.248, and ESET Nod32 Smart Security. The study's findings indicated that personal firewalls are not user-friendly, which could result in security vulnerabilities. The usability issues may be attributed to the firewalls' unclear or deceptive information during installation, configuration, or interaction. There are numerous usability issues associated with the diminished clarity of warnings. Li [8] investigated the challenges associated with incorporating firewalls into the architecture of networking layouts and the optimization of routing tables to ensure that a firewall's code set is as compact as possible while still being highly effective. This prevents the formation of speed bottlenecks and seals security vulnerabilities. Furthermore, two significant contributions have been made: demonstrating that the problems are NP-complete and devising a heuristic solution. Additionally, simulations have been implemented to demonstrate the effectiveness of algorithms. The test results indicate that the recommended approach has fewer rules for multiple firewalls than other algorithms.

• Sudha Rani et al. [18] conducted vulnerability assessment studies to investigate the methods by which intrusion detection systems (IDS) identify when a computer network is under attack. In order to prevent the vulnerability of a network of virtual devices, it is recommended that a system be implemented to detect intrusions. The investigation also examined potential security risks and the considerations that must be taken into account when establishing a private virtual network [16, 15]. The study's findings indicate that there are two distinct categories of intrusion monitoring systems: network-based and host-based. Additionally, the proposed solution outlines strategies for leveraging the adaptability of program transitions to enhance the accuracy of detection and the capacity to overcome them. Another study [4] concentrated on the assessment of vulnerability for automatic environments, web applications, and various hazards identified during the vulnerability examination of diverse networking products. The study employed the OpenVAS instrument and a research methodology known as "exploratory research." The study's findings suggested that the PHP info method and other methods, such as Trojan, can be employed to resolve vulnerabilities and eliminate hazards. This contributes to the security of networking systems. The cyber security quantitative risk assessment model for DAS was examined by Ye et al. [25]. The review process is divided into three components: the development of a vulnerability adjacency matrix, the simulation of the operation of attacks, and the examination of the physical consequences. As actual power systems become increasingly integrated with cyber systems, cyber security issues are exacerbated. In comparison to other controllers in electrical substations or power plants, DAS is significantly more vulnerable to hacker attacks.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14220

However, it is responsible for ensuring that each and every DAS is safe, not beneficial for business, and not technically necessary. The theory recommends the development of ADG models, the identification of potential physical consequences of cyberattacks, and the provision of a vulnerability adjacency matrix to illustrate the interconnections between various vulnerabilities. There are numerous case studies that demonstrate the effectiveness and validity of the vulnerability assessment model that has been proposed as a result of the RBTS bus 2.

V. PROACTIVE APPROACHES TO CYBERSECURITY DÉFENSE

- **Understanding the Threat Landscape**: The first step in building a strong defence is recognizing the evolving nature of cyber threats. This includes understanding common attack vectors such as phishing, malware, ransomware, and insider threats. Acknowledging these threats allows organizations to tailor their prevention strategies accordingly.

- **Establishing Security Policies**: Organizations should develop and enforce clear cybersecurity policies that outline acceptable use, data handling practices, and security protocols. These policies serve as a framework for ensuring that all employees understand their roles and responsibilities in maintaining security.

- **Regular Software Updates and Patching**: Keeping software, operating systems, and applications up to date is essential for mitigating vulnerabilities. Organizations should implement a routine schedule for software updates and patch management to address known security flaws.

- **Employee Training and Awareness**: Human error is often a significant factor in cybersecurity breaches. Regular training sessions and awareness programs can equip employees with the knowledge to recognize phishing attempts, understand the importance of password hygiene, and follow security protocols.

- **Protecting your passwords:**

– Don't tell anyone what your passwords are, and make new ones that are hard to figure out. Avoid words from dictionaries and make a password with a mix of numbers, letters, and symbols.
– Don't use popular passwords like xyz567, (your name), favoritebook1, cricket1, or their variations.
– Change your passwords every so often.
– When picking a password, do the following:
– Use a mix of capital and lowercase letters.
– Use at least 8 characters.
– Use symbols to remember a hard password.

- **Running anti-virus programs**

– To avoid computer virus problems, install and run anti-virus software like Sophos and check when it was last updated.
– It's important to check every so often to see if the antivirus software you have loaded is up-to-date. This helps block both present and future viruses. The anti-virus software gets rid of viruses, puts them in quarantine, and then fixes infected files on the user's machine. Students, staff, and teachers at UC Davis can get the Internet Tools CD from the Shields Library's IT Express and use it to get free Sophos software for their home and work computers.

- **Preventing ID Theft**

– Don't give out your bank card numbers, social safety numbers, driver's license numbers, or other private data unless you know who it's going to. Protect the details of other people as you would protect your own.
– Don't send private or sensitive information through email or chat messages because it's easy for people to read them.

– Watch out for phishing scams, which try to get your private or banking account information by sending emails that look like they came from a reliable business (often a bank). Most of the time, these don't have a handwritten greeting. Never put sensitive data into a website's form you got through a link or an email from an email address you don't know. Online, most real businesses don't ask for personal information.

VI. FUTURE DIRECTIONS

Here are some potential future directions based on the themes and findings from your paper on contemporary challenges in cybersecurity:

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14220

Future research could concentrate on the development of more user-friendly and robust password management systems, in light of the identified lacuna in password security studies. This encompasses the development of mechanisms that enforce stringent password policies and the investigation of innovative authentication methods, such as biometric authentication or multi-factor authentication (MFA).

• **Integration of AI and Machine Learning:** Examine the function of artificial intelligence (AI) and machine learning (ML) in improving cybersecurity measures. Research could investigate the potential of AI-driven solutions to automate threat detection, response, and mitigation strategies, thereby enabling real-time analysis of potential vulnerabilities and attacks.

•**User-Centric Cybersecurity Education:** Investigate the efficacy of user-centric cybersecurity education programs that cater to a diverse range of demographics, such as employees, consumers, and small business proprietors. Future research could assess the influence of customized training on the reduction of human error incidents and the enhancement of cybersecurity awareness.

•**Cybersecurity in the Internet of Things (IoT)**: Research could explore the specific cybersecurity challenges that IoT devices present in light of their increasing adoption. It would be imperative to investigate frameworks for securing IoT ecosystems and establish standards for device manufacturers in order to improve the overall cybersecurity posture.

• **Regulatory Compliance Frameworks:** Analyze the influence of changing regulations, such as GDPR, on cybersecurity practices within organizations. Future research could suggest frameworks that assist organizations in efficiently navigating compliance while assuring the implementation of robust data protection and cybersecurity measures.

Researchers can contribute to the ongoing endeavors to improve cybersecurity in an increasingly complex and digital landscape by investigating these future directions.

VII. CONCLUSION

This paper has emphasized the vital importance of cybersecurity in the changing realm of e-commerce and social commerce, where the incorporation of digital technology has revolutionized corporate processes and client engagements. With the growing dependence of enterprises on online platforms for transactions, they are confronted with a wide range of cyber dangers, such as malware, ransomware, phishing attempts, and the spread of false information, which can erode consumer trust. The systematic examination of current literature highlights a deficiency in specialized research on password security, which continues to be a fundamental component of cybersecurity measures. The results suggest that although there have been notable improvements in email security and firewall protection, there is an urgent requirement to investigate password management solutions and user-focused methods to cybersecurity education. The existing recommendations for password security do not include strict methods to ensure effective implementation. This highlights the need for novel solutions like biometric authentication and multi-factor authentication (MFA). Furthermore, the article highlights the significance of thorough cybersecurity frameworks that tackle the particular difficulties presented by emerging technologies such as the Internet of Things (IoT) and the intricacies of regulatory compliance. In order to safeguard sensitive information and maintain uninterrupted business operations, firms must use proactive measures to counter the ever-changing techniques of cybercriminals. Ultimately, the need for strong cybersecurity measures is more evident than ever. Subsequent investigations should prioritize the creation of efficient password security methods, augmenting user awareness and education, and investigating the incorporation of artificial intelligence and machine learning in cybersecurity activities. By giving priority to these areas, researchers and practitioners may help create a more secure digital environment, promoting trust and safety for both businesses and consumers**.**

Competing Interest:
- The author has no competing interests to declare that are relevant to the content of this article.
- The author declare that they have no conflict of interest.

Author Contribution Statement:
- Amandeep Kaur examines the technique and compiles the main research work.

Ethics and informed consent for data used
- The author has no relevant financial or non-financial interests to disclose.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14220

- The author certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.
- The author has no financial or proprietary interests in any material discussed in this article.
- This article does not contain any studies with human participants or animals performed by the author.
- This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data Availability and access: There is no research data to declare.

REFERENCES

[1]. A. Tonge, S. Kasture, and S. Chaudhari. Cyber security: challenges for society-literature review. IOSR Journal of Computer Engineering, 2(12):67–75, 2013.
[2]. Adlakha, R., Sharma, S., Rawat, A., & Sharma, K. (2019). Cyber Security Goal's, Issue's, Categorization & Data Breaches. Paper presented at the 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon).
[3]. Ahmed, M. Elsholkami, A. Elkamel, J. Du, E. Ydstie, and P. Douglas. Financial risk management for new technology integration in energy planning under uncertainty. Applied Energy, 128:75–81, 2014.
[4]. B. Alfayyadh, J. Ponting, M. Alzomai, and A. Jøsang. Vulnerabilities in personal firewalls caused by poor security usability. In IEEE Int'l Conf. on Infor. Theor. and Infor. Security, pages 682–688, Beijing, China, 2010. IEEE
[5]. Burton, W. (2007). *Burton's legal thesaurus*, 4 Edn. New York, NY: McGraw-Hill Education.
[6]. F. Hu, M. Qiu, J. Li, T. Grant, D. Taylor, and S. McCaleb et al. A review on cloud computing: Design challenges in architecture and security. J. of Computing and Info. Tech., 19(1):25–55, 2011.
[7]. F. Liu, H. Lo, L. Chen, and W. Lee. Comprehensive security integrated model and ontology within
[8]. J. Li. The research and application of multi-firewall technology in enterprise network security. Int'l J. of Security and Its Applications, 9(5):153–162, 2015.
[9]. Jennifer. (2022). *Top E-commerce challenges facing SMBs. business news daily.* Availble online at: https://www.businessnewsdaily.com/6028-small-ecommerce-challenges.html
[10]. K. Gai and S. Li. Towards cloud computing: a literature review on cloud computing and its development trends. In 2012 Fourth Int'l Conf. on Multimedia Information Networking and Security, pages 142–146, Nanjing, China, 2012
[11]. K. Gai, M. Qiu, L. Chen, and M. Liu. Electronic health record error prevention approach using ontology in big data. In 17th IEEE International Conference on High Performance Computing and Communications, pages 752–757, New York, USA, 2015.
[12]. Khurana, A. (2019). *"Did You Know That There Are 4 Types Of Ecommerce?". The Balance Small Business*. New York, NY: Dotdash.
[13]. Koomey, J. (2012). *The benefits of information technology outweigh the costs.* New York, NY: The New York Times.
[14]. M. Qiu, H. Su, M. Chen, Z. Ming, and L. Yang. Balance of security strength and energy for a PMU monitoring system in smart grid. IEEE Communications Magazine, 50(5):142–149, 2012
[15]. M. Qiu, L. Zhang, Z. Ming, Z. Chen, X. Qin, and L. Yang. Securityaware optimization for ubiquitous computing systems with SEAT graph approach. J. of Computer and Syst. Sci., 79(5):518–529, 2013.
[16]. M. Qiu, W. Gao, M. Chen, J. Niu, and L. Zhang. Energy efficient security algorithm for power grid wide area monitoring system. IEEE Transactions on Smart Grid, 2(4):715–723, 2011.
[17]. Mishra, A., Alzoubi, Y. I., Gill, A. Q., and Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors* 22:538. doi: 10.3390/s22020538
[18]. N. Rani, A. Satyanarayana, and P. Bhaskaran. Coastal vulnerability assessment studies over india: a review. Natural Hazards, 77(1):405– 428, 2015.
[19]. O. Boric-Lubecke, X. Gao, E. Yavari, M. Baboli, A. Singh, and V. Lubecke. E-healthcare: Remote monitoring, privacy, and security. In IEEE Int'l MTT-S, pages 1–3, Tampa, FL, USA, 2014.
[20]. Raghavan, K., Desai, M. S., & Rajkumar, P. (2017). Managing cybersecurity and ecommerce risks in small businesses. Journal of management science and business intelligence, 2(1), 9-15.
[21]. Reynolds, J. (2000). eCommerce: a critical review. *Int. J. Retail Distrib. Manage.* 28, 417–444. doi: 10.1108/09590550010349253
[22]. S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1):1–11, 2011.
[23]. Thomas, J. (2016). *Systems theoretic process-analysis STPA.* Availble online at: http://psas.scripts.mit.edu/home/wp-content/uploads/2016/01/

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14220

[24]. Wang, Z., Li, M., Lu, J., and Cheng, X. (2022). Business innovation based on artificial intelligence and blockchain technology. *Inf. Process. Manage.* 59:102759. doi: 10.1016/j.ipm.2021.102759

[25]. X. Ye, J. Zhao, Y. Zhang, and F. Wen. Quantitative vulnerability assessment of cyber security for distribution automation systems. Energies, 8(6):5266–5286, 2015.

[26]. Y. Badr, F. Biennier, and S. Tata. The integration of corporate security strategies in collaborative business processes. IEEE Trans. on Services Computing, 4(3):243–254, 2011.

[27]. Yibin Li, Wenyun Dai, Zhong Ming, and Meikang Qiu. Privacy protection for preventing data over-collection in smart city. IEEE Transactions on Computers, PP(99):1, 2015.