IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Comparative Analysis Of The Data Privacy And Security In E-Commerce Sites

[1]Hakim Burhanoddin Akram, [2]Sakshi Deepak Pawar, [3]Sejal Digambar Wakchaure

[1]Assistant Professor, [2]Student, [3]Student

[1]Department of Mathematics,

[1]Dr. D. Y. Patil, Arts, Commerce & Science College, Pimpri,

Pune, Maharashtra, India

Abstract:

Nowadays e-commerce platforms are growing rapidly; a number of people visit websites and also use them. On the other side data, privacy and security challenges also increase. If these privacy and security challenges are not resolved, consumers can never trust or visit any e-commerce websites. This study provides a comparative analysis of the data security and data privacy in traditional and modern digital system. It gives a detailed evaluation of different aspects of data privacy and issues related to its implementation. It also examines the need to secure the personal data of the users and the frequent security concerns that online business encounter. This paper also examines strategies that are helpful for users to stay safe in the digital era by taking security precautions. The results have shown that the efficiency of modern security solutions, their scalability and ability to detect threats real-time are better than the traditional approaches, but modern solutions have also brought privacy and data transparency challenges. Recent cybersecurity statistics establish the validity of the analysis and provide an understanding of the need to develop advanced security frameworks to tackle the rapidly increasing cyber threats.

Keywords: Data security, E- commerce, E- commerce privacy

Graphical abstract:

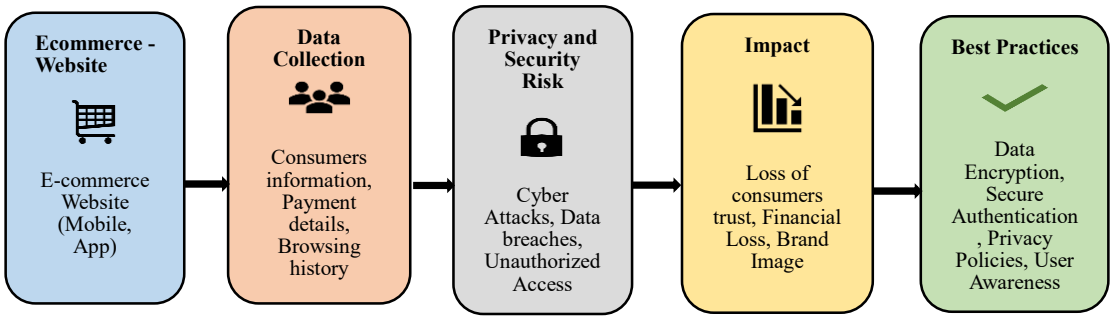

figure 1: data privacy and security in e-commerce website

1.INTRODUCTION

In recent times, E- commerce business have been grown rapidly; consequently, challenges related to data privacy also arise. As a result, consumers will not trust and avoid visiting the e-commerce platforms. An E- commerce platform's success and user trust largely depends on its security and privacy measures. Building a trust among consumers is essential for growth of the business.

The term E- commerce describes purchasing and selling products or services. It involves technologies like mobile apps, digital payment processes, supply chain management and collection of sensitive user data. Even though we need this data to enhance user experience, personalization, operational performance, it also increases vulnerability of cyberattack, and abuse of personal information. E- commerce is the popular and fastest growing sector of the electronic industry.

Over recent years, the internet technologies have been widely used in the commerce sector. Lots of offline retailers and wholesalers are moving to e-commerce platforms to connect with more consumers and improve their business. Although e-commerce has several benefits, it also poses serious security issues that have the potential of compromising the security of customers. Day by day the level of digital literacy is increasing, lots of people use digital devices daily and users trust online platforms blindly without proper awareness. Due to this, users personal and confidential data being accessed and misused without their permission. Organization started using multiple security mechanisms such as encryption techniques, authentication controls, monitoring systems, and legal rules to reduce risks. Even with these security efforts, data breaches still occur due to weak security practices, lack of transparency, third-party risks, and increasing cyber threats. This paper discusses privacy and security concerns in e-commerce and how it affects consumers and businesses. It also introduces the comparative analysis of the classical and modern data security methods, and the measures of the best practices that can be undertaken to improve the data protection, and the assurance of the online transactions.

1.1 OBJECTS OF THE STUDY

The objects of this study are as follows:

- To examine data privacy and security problems in E-commerce websites.
- To analyze the major causes and different types of data breaches occur in E-commerce.
- To identify limitations in present security systems implemented by e-commerce websites.
- To highlight the effective practices and preventive measures for enhancing data privacy and security in e-commerce platforms.
- To conduct a comparative study of conventional and innovative data protection methods.

1.2 ORGANIZATION OF THE ARTICLE

This paper organized are as follows:

Section 1: Introduction, objectives, and structure of the paper.

Section 2: Reviews relevant literature on data privacy and security challenges in e-commerce.

Section 3: Explain the research methodology and comparative framework.

Section 4: Reports the analysis and discussion findings.

Section 5: Conclusion summarizing key findings and future scope.

2.LITERATURE REVIEW

This segment of the paper survey on the existing literature about the issues of data privacy and security in the context of e-commerce platforms and appends a basis on the current comparative analysis.

Initial trends in e-commerce security:

The online business started with the emergence of massive online purchases in the 1990s with the development of e-commerce business models like Amazon and eBay. Early forms of security mostly depended on simply encrypted methods of transmission like the Secure Scope Layer (SSL) protocols to secure payment details. But, because of the lack of a sufficient level of cybersecurity awareness and ineffective authentication mechanisms, users were exposed to fraud, phishing and data breaches.

Development of high-level Security Technology:

As the number of digital transactions grew fast in the 2000s to 2010s, even advanced security mechanisms were implemented. The end-to-end encryption, multi-factor authentication, safe payment gateways and fraud detection algorithms became typical of the leading e-commerce websites. With the emergence of international data protection laws, such as the general data, protection regulation, privacy compliance requirements were tightened. Besides, the emergence of cybersecurity systems and risk management paradigms resulted in enhanced security against identity theft, financial fraud, and unauthorized access to data.

Data Privacy in the age of big data and AI:

The introduction of big data analytics and artificial intelligence into the platforms of e-commerce changed the approaches to the collection and processing of data greatly. The use of personalized recommendations, targeted advertising and predictive analytics has improved the user experience, however, there were concerns of over collection of data and profiling of the users. Recent reports note that the risks connected to the third-party data sharing, vulnerability of cloud storage, and cross-border data transfers are increasing, and it is necessary to simplify the privacy policies and enhance the user consent mechanisms.

Security Challenges in Traditional Authentication Systems:

Past works indicate that the conventional authentication systems depend on identify-based access control system, which is many cases, is very powerful in terms of computation during the encryption and authentication of identity. This poses a problem in efficiency and scalability particularly in peer-to-peer (P2P) e-commerce setup. As such, advancements in authentication systems and streamlining of encryption algorithms have become a major area of concern towards raising security levels in online transactions. Also, the expansion of e-commerce, especially in the banking industry, brings in new risks and weaknesses with regard to cybersecurity attacks. The information security is crucial since the online payment transaction must be provided with a high level of security, but it is a complicated issue because of the constant technological progress and new business demands, which demand the combination of powerful algorithms and precise technical solutions.[11]

Comparison of Current research (2020-25):

The recent studies of 2020-25 have been comparing the traditional security instruments and the AI-based cybersecurity tools. The AI-based fraud detection systems have proven more accurate and quicker to identify threats then the conventional rule-based systems. But there are also reports that advanced cyberattacks such as ransom and social engineering remain a challenge to what is in place as defense mechanisms. Moreover, consumer trust is also at stake not just by technological protection but also by regulatory conformance and company transparency.

Literature Gaps:

There are still some gaps in literature in spite of the negative technology changes. There are few empirical studies on the effectiveness of security strategies over a long term in a real-world environment of e-commerce. Consumer awareness and consumer behavioral response to privacy policies also lack enough

studies. In addition, the ethical issues of data monetization, surveillance operations, and algorithmic bias also need to be studies. The existence of these gaps points out the necessity to carry out through comparative research to assess data privacy and security frameworks based on their effectiveness, transparency, and consumer protection.

3.METHODOLOGY

This paper is a comparative research project in which it focuses and analyzes various methods employed to guarantee the security and confidentiality of data on online systems. The study aims at the comparison of traditional data protection mechanisms with new technological solutions like artificial intelligence (AI) based security, blockchain technology and cloud security frameworks. The main aim is to examine the strengths, weaknesses and the general effectiveness of such methods in guarding classified information. Through a systematic analysis of the literature and records of past case studies, this methodology will seek to establish a holistic perspective of how the emerging technologies are changing the management of data security and privacy.

Research Design and Approach

The research design is a qualitative research design that is backed by secondary data analysis. The study does not involve primary experiments but uses the information published and tried by other scholars and industries which are reliable and valid. This method will enable the research to investigate several viewpoints and finding that were realized in different researches within the field of cybersecurity. A review of many peer-reviewed journal articles, conference papers, industry reports, cybersecurity frameworks, and case studies have been published 2020-25. It is within this timeframe that the research has been chosen to allow the research to capture the most recent developments and changing threats in the area of data protection and privacy technologies.

Areas of Comparative Analysis

The comparative analysis is based on various areas that are most critical in terms of data privacy and data security.

1. Techniques of Data Encryption and Data Protection: This area examines the manner in which data is secured by application of encryption algorithms, cryptographic protocols and secure data storage.
2. Authentication and Authorization: Authentication process are used to guarantee access to sensitive data by the right individuals. The analysis makes the comparison of the conventional systems of password-based authentication with multi-factor authentication, biometric authentication, and identity verification methods that are driven by AI.
3. Information Security and Laws and Regulations: Companies should follow the privacy laws and ethical principle in processing personal information.
4. Threat Detection and Prevention of a cyberattack: These are cyber threats which include malware attacks, phishing activities and data breaches which are very dangerous to information systems. This field takes into consideration the performance of the traditional security monitoring system in comparison to AI-powered threat detection and predictive cybersecurity solutions.
5. Privacy and Confidentiality of the users: This field explores the security of various systems in safeguarding personal data, confidential documents as well as sensitive digital identities to make sure that data is utilized in a manner that is ethical and responsible.

Evaluation Criteria

Individual domains are measured on the following basis:

- **Security Effectiveness:** Capability of the system to respond to unauthorized access, cyberattacks, and data breach of information.
- **Scalability:** Ability of the system to support extra data, users and transactions without compromising on security performance.
- **Operational Efficiency:** Security mechanisms performance regarding processing speed, system efficiency and usage of resource.
- **Protection of Privacy:** Effectiveness in protecting personal data, sensitive data and identities of the users.
- **Cost Efficiency:** Organizational and user security solution implementation and maintenance.
- **Flexibility to New Threats:** Capacity of security systems to adapt to new cyber threats and new methods of attack.

Data Sources

The analysis is done on the basis of the data gathered on a variety of trusted sources such as:

- Academic databases like IEEE Xplore, Scopus, ACM Digital Library and ScienceDirect which are peer-reviewed.
- The organization like the National Institute of Standards (NIST), ISO offer cybersecurity frameworks and standards.
- Case studies and research results in the well-known cybersecurity and information security journals.
- Released industry reports, technical documentation, and white papers of the major technology companies that include Microsoft, IBM, Cisco.
- Cybersecurity statistics and reports were released by the Indian Computer Emergency Response Team (CERT-In).

Analytical Procedure

The comparative study was carried out in a multi-step process that are structured in these ways:

1. Relevant Literature Identification: Keywords were used to identify the relevant research papers, reports, and articles; the keywords used included data security, data privacy, cybersecurity structures, encryption methods, and privacy security technologies.
2. Filtering and vetting of Sources: The sources obtained were checked and filtered to consists of credible peer-reviewed and relevant sources related to the topic of research.
3. Key Information extraction: The key information regarding security measures, privacy models, system performance, and threat reduction strategies were revealed in the chosen literature.
4. Formulation of Comparative Framework: An organized framework was created that would compare the old methods of data protection with the advanced security technologies on the basis of the chosen evaluation criteria.
5. Organization of Findings Thematically: The information that was extracted was grouped into thematic areas which included encryption, authentication, privacy protection and threat detection.
6. Interpretation and Synthesis: The last phase entailed the interpretation of the evidence obtained and taking a synthesis of the results to conclude on the overall performance and shortcomings of different data security and privacy strategies.

4.RESULT AND DISCUSSION

4.1 COMPARATIVE RESULT:

The comparative analysis of the conventional data security methods and the current technology-based security solutions in main fields like data protection, detection of threats, access controls security management have revealed their differences. The results that contemporary security solutions enhance security performance, efficiency, and scalability, and present issues associated with data privacy and openness.

Regarding data protection, the traditional systems are limited to simple encryption and human touch but the new systems are advanced as they offer high-end encryption and automated security protocols to increase the safety of data. In detecting threats, the older systems rely on the rule-based monitoring and the newer systems utilize the AI-based detection and act promptly.

Concerning the authentication, the conventional password-based systems are more susceptible compared to the current systems that apply multi-factor authentication and biometric verification that enhances the security. In a similar fashion, the current cloud-based application like Microsoft-Azure, have automated security management that eliminates manual work and enhances operational efficiency.

All in all, contemporary data security systems have better efficiency and flexibility in comparison to older systems, but must have the privacy and ethical issues well controlled. These comparisons are summarized in table 1.

COMPARATIVE TABLE:

table 1: traditional security vs ai based security in e-commerce

Factors	**Conventional Security Controls**	**AI-Based Security in E-commerce**
Security Strategy	Rule based systems and simple encryption	Threat detection and predictive security models based on AI
Fraud Detection	Manual checking and set rules to identify suspicious activity	Machine learning-based real-time fraud detection
Data Protection	Simple encryption using the basic version of the SSL and restricted tracking of data	Encryption, tokenization, and sophisticated cybersecurity systems
Authentication	Password based authentication	Multi-factor biometric authntication
Response to Threats	Reactive strategy when a security breach has taken place	Active Strategy, prediction risks early and utilizing automatics to provide alert systems
Privacy Control of the users	Less visibility on the data usage policies	Improved privacy privileges and compliance protocols
Problems	Time-consuming threat detection and increased threats of data breach	Data privacy, expensive infrastructure and reliance on complex technology

4.2 DISCUSSION:

It has been found that online users tend to trust and believed in transacting online when the websites offer high level of security, explain their privacy and data protection practices clear because these elements mitigate privacy-related doubts in the minds of online users. Conversely, websites with poor security, ambiguous policies, or non-disclosed data sharing policies are likely to defer site users to provide personal information, and as a result, their privacy issues intensify, and their total level of confidence diminishes. [8]

The current technologies are making use of AI-based security systems and cloud-based platforms, which are more efficient in dynamic environments as they enhance threat detection and response ability. Nonetheless, the embrace of the technologies also raises issues that deal with data privacy, transparency, and also ethical use of information. Hence, organizations should strike a balance between the security development and effective privacy policy to ensure the user trust.

The findings suggest that there is a big contrast between the traditional and modern data security strategies. The vulnerability of the digital systems is evident in the rising tread of the cyber incidents. This indicates that customary security solutions cannot be used to deal with sophisticated cyber threats.

Following chart shows the number of data breach reported to and handled by CERT-in

table 2: data breaches

Year	Total incidents reported/handled
2019	3,94,449
2020	1,158,208
2021	1,402,809
2022	1,391,457
2023	1,592,917
2024	2,041,360
2025	2,944,000

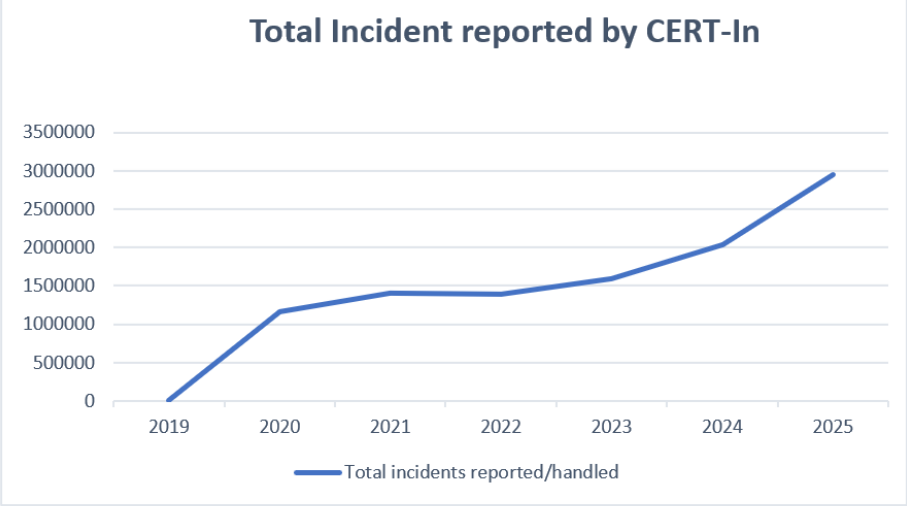

Figure 1 : total incident reported by CERT-In

5.CONCLUSION :

This paper gives a comparative study of the data protection and confidentiality in e-commerce with the emphasis of the distinctions between the conventional and advanced security methods. The result indicate that even traditional approaches offer the minimum of protection but many of them fail to meet the growing sophistication of cyber threats. The current security solutions have advance features in efficiency, scaling abilities, and the advanced threat detection. Nevertheless, these technologies also involve problems regarding data privacy, information transparency and moral use of information. In general, this research determines that the use of a balanced strategy that incorporates both highly

developed security tools and highly developed privacy regulations provides the answer to secure and reliable online transactions.

6.FUTURE SCOPE :

The further studies may be directed towards the creation of more sophisticated and dynamic security mechanisms in order to meet the new cyber threats. Data protection and privacy in the e-commerce sites can be further improved with the integration of technologies like artificial intelligence, blockchain, and zero-trust security models. Further research can as well be done on how the user awareness and behavior about the data privacy that is very important in ensuring the secure online environments. What is more, enhancing transparency, minimizing the impact of algorithms, and making a data usage ethical process will continue to yield future research in data security and privacy.

REFERENCES

[1] Muneer, A.; Razzaq, S.; Farooq, Z 2018, Data Privacy Issues and Possible Solutions in E-commerce. *J. Account. Mark. 7*, 294.

[2] Chandrakanth Reddy Borra 2022, A Comparative Study of Privacy Policies in E-Commerce Platforms, International Journal of Research and Applied Innovations (IJRAI), Volume 5, Issue 3.

[3] Indian Computer Emergency Response Team, "Cyber Security Incident Reports," Ministry of Electronics and Information Technology, Government of India, 2023. [Online]. Available: https://www.cert-in.org.in

[4] Microsoft, "Security and privacy in the age of AI," Microsoft, 2023. [Online]. Available: https://www.microsoft.com/security

[5] Microsoft, "Microsoft Azure security documentation, Microsoft Azure, 2023. [Online]. Available: https://azure.microsoft.com

[6] Zlatan Morić*, Vedran Dakic, Daniela Djekic and Damir Regvart 2024, Protection of Personal Data in the Context of E-Commerce" Journal of cybersecurity and Privacy, vol.4(3),731-761.

[7] Arora, D. Data Privacy Issues with E-Commerce. *Int. J. Soc. Sci. Econ. Res.* 2023, *8*, 1167–1174.

[8] Mahmood H Shah, Ramanus Okeke, Rizwan Ahmed, 2013, Issues of Privacy and Trust in E-Commerce: Exploring Customers' Perspective, J. Basic. Appl. Sci. Res., 3(3)571-577.

[9] Dhruv Arora 2023, DATA PRIVACY ISSUES WITH E-COMMERCE, International Journal of Social Science and Economic Research, ISSN: 2455-8834, Vol 8.

[10] Srinivasan, S. 2015, Privacy protection and data breaches, Proceedings of informing Science & IT Education Conference (InSITE), 429-444.

[11] Niranjanamurthy M, DR. Dharmendra Chahar 2013, The study of E-Commerce Security Issues and Solutions ,nal Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7.