International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *10 September 2023* ***Revised:*** *14 October 2023* ***Accepted:*** *28 October 2023*

Modeling and Validating Structural Relationship among Customer Data Privacy in E Commerce and Data Breaches.

Dr. Deepti Lele
Adjunct Faculty
Department of Management Studies
COEP Technological University
deeptilele.coep@gmail.com

Abstract:

This abstract provides an overview of a comprehensive study aimed at modeling and validating the structural relationships between customer data privacy practices in e-commerceplatforms and the occurrence of data breaches. This research bridges the gap in understandinghow the level of investment and adherence to data privacy measures in e-commerce businesses influences the likelihood and severity of data breaches.The study employs amixed-methods approach, combining quantitative analysis of large-scale data sets related to e-commerce platforms and data breach incidents with qualitative analysis of privacy policies, regulatory frameworks, and industry best practices.

Key words- Customer, Data Privacy , CSF, Data Breach, E commerce, Data Breach.

Objectives

Modeling Data Privacy Practices: A structural model is developed to analyze the relationships between various dimensions of customer data privacy practices in e-commerce, including data encryption, user consent, data anonymization, and compliance with privacy regulations.

Quantifying Data Breach Incidents: By collecting and analyzing data breach incidents reported in e-commerce, the research assesses the frequency, scale, and nature of data breaches.

Validation of Relationships: Statistical techniques such as regression analysis and structural equation modeling are applied to validate the structural relationships between data privacy practices and data breach incidents.

Impact Assessment: The study assesses the potential economic, reputational, and legal impacts of data breaches on e-commerce businesses and their customers.

Recommendations: Based on the findings, the research offers recommendations for enhancing data privacy practices in e-commerce, including actionable insights for businesses, policymakers, and regulatory bodies. This research contributes to the growing body of knowledge on the critical intersection of data privacy and data breaches in the e-commerce sector. By understanding the structural relationships between these factors, stakeholders can proactively implement strategies to safeguard customer data and mitigate the risks associated with data breaches, ultimately fostering trust and confidence in e-commerce platforms.

Introduction

Data privacy and security have emerged as crucial concerns for both consumers and businesses in the fast changing e-commerce environment. The rapid growth in online transactions has resulted in a significant rise in the gathering and handling of client data, hence increasing the likelihood of data breaches. To address this situation, it is essential to have a comprehensive comprehension of the interconnection between client data privacy in online business and the incidence of data breaches. It is essential to model and validate these linkages in order to create successful tactics that reduce risks and improve consumer trust.

This introduction highlights the need of representing the complex structural connections between client data privacy and data breaches in the e-commerce industry. It highlights the necessity for comprehensive and dynamic models that can

precisely depict the intricate interaction of multiple elements influencing these relationships. The primary objective will be to ascertain crucial factors, such as methodologies for gathering data, policies on privacy, measures for ensuring security, and patterns of consumer behaviour, and to comprehend their interplay in influencing the probability and consequences of data breaches.

The major goal of this modelling endeavour is to offer valuable insights on how e-commerce enterprises can enhance the security of client data, adhere to ever-changing data privacy requirements, and uphold consumer confidence. By verifying these models using empirical data and real-world scenarios, it becomes feasible to detect potential vulnerabilities, predict the probability of data breaches, and develop proactive tactics to prevent them.

Moreover, this introduction will examine the consequences of these models for policy-makers, corporations, and consumers. It will emphasise the significance of a cooperative strategy that includes all parties involved in tackling the difficulties of data privacy and security in electronic commerce. The primary objective is to cultivate a setting in which consumer data is both securely protected and ethically and responsibly utilised, thereby guaranteeing the long-term viability and expansion of the e-commerce sector in a data-centricsociety.

Related work

Surjandy, et al. (2022): The authors of the study titled "Analysis of Data Quality and Data Privacy Factors on the Factors of Intention to Buy and Decision to Buy on e-Commerce during Pandemic COVID-19" presented their findings at the 2022 International Conferenceon Information Management and Technology in Semarang, Indonesia. The study focuses on examining how data quality and privacy impact consumer behaviour in e-commerce during the COVID-19 pandemic. They provide valuable information on how data-related aspects influence the intention to purchase and the ultimate decision-making process. Their study is especially pertinent in comprehending consumer behaviour in a world impacted by a pandemic.

Shejy et al. (2022): The authors of the article "Sensitivity Support in Data Privacy Algorithms", given at the 2022 2nd Asian Conference on Innovation in Technology in Ravet, India, aim to improve data privacy algorithms by incorporating sensitivity support. This task is essential for the development of strong privacy-preserving methods in data management, especially in situations when data sensitivity is of utmost importance.

Perumal, et al. (2019): Their study, titled "Proposed Customer's Sensitive InformationPrivacy Model for Financial Institution," presented at the 2019 International Conference on Computing, Electronics & Communications Engineering in London, introduces a novel framework for safeguarding confidential customer data in financial institutions. This study is crucial in establishing a structure for protecting client data in the financial industry, emphasising the equilibrium between data usefulness and confidentiality.

Li, Yumeng, et al. (2016): The article, entitled "Anonymity-based data publishing for preserving customer privacy in railway systems", examines the difficulties associated with safeguarding customer privacy within the framework of railway systems. It was presented at the 2016 IEEE International Conference on Intelligent Rail Transportation in Birmingham. Their methodology for implementing anonymity-based data publishing makes a noteworthy impact on the domain of data privacy in public transport systems.

Wang et al. (2022): In the research paper titled "Big Data Analysis and Mining Technology of Smart Grid Based on Privacy Protection", which was presented at the 2022 6th International Conference on Computing Methodologies and Communication in Erode, India, Wang highlights the importance of safeguarding privacy while analysing and mining large datasets in smart grid systems. This work is essential for comprehending privacy implications in the swiftly developing field of smart grid data analysis.

We will do a comprehensive study of the required research papers, categorising the contentinto sections such as Citation, Methods, Advantages, Disadvantages, and Research Gaps.

Proposed methodology

The swift expansion of e-commerce has resulted in a significant surge in the gathering and retention of user data. Although this data is crucial for businesses to function efficiently, it also poses a substantial threat of data breaches[5]. Data breaches might result in severe repercussions for both enterprises and individuals, encompassing monetary setbacks, harm to reputation, and legal accountability.

To minimise the likelihood of data breaches, firms must comprehend the inherent connections between client data protection and data breaches. This comprehension can be utilised to develop efficient data security rules and protocols[6].

This study presents a methodology for creating and verifying the structural connections between client data privacy in e-commerce and data breaches. The approach comprises the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 10 September 2023 **Revised:** 14 October 2023 **Accepted:** 28 October 2023*

subsequent steps:

Data Collection: Gather information on consumer data privacy practises, data breach events, and other pertinent elements from diverse sources, including industry reports, academicresearch, and government databases.

Table 1: The dataset table used for modelling and validating the structural links between client data privacy in e-commerce and data breaches consists of multiple components. Below is an illustration of a possible arrangement for organising such a table:

Column Name	Data Type	Description
Customer_ID	Integer	An individual customer ID
Age	Integer	Customer age
Gender	String	Customer gender
Location	String	Customer geography
Purchase_History	String/JSON	Purchase history of client
Payment_Method	String	Credit card, PayPal, etc.
Data_Sharing_Consent	Boolean	Whether customers consent to data sharing
Privacy_Settings	String	Customer privacy settings on the e-commerce platform
Account_Creation_Date	Date	Customer account creation date
Last_Login	Date	Latest login date
Data_Breach_Incident	Boolean	Provides information about data breaches involving customers.
Data_Breach_Date	Date	Date of data breach, if applicable
Data_Breach_Type	String	Data breach kind (hacking, phishing,etc.)
Breach_Severity	Integer/String	How severe the breach is
Reported_Damages	Float	Customers' breach-related losses in dollars
Changed_Privacy_Settings_Post_Breach	Boolean	Reports whether the customer altered their privacy settings following the breach.
Trust_Score	Float	A post-breach score of client trust in the e-commerce platform

This table is versatile and may be utilised for a range of analysis, including examining the relationship between consumer demographics and the probability of data breaches, as well as investigating the impact of data breaches on customer behaviour[7] and faith in e-commerce platforms. Every row in the database corresponds to a distinct consumer, while the columns contain pertinent information regarding their interactions with the e-commerce platform,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *10 September 2023* ***Revised:*** *14 October 2023* ***Accepted:*** *28 October 2023*

theirpersonal data, and any instances of data breaches[8].

Data Preprocessing: Data preprocessing involves the meticulous cleaning and preparation of the data for analysis. This includes the removal of missing values[9], outliers, and inconsistencies.

Exploratory Data Analysis: Exploratory Data Analysis involves examining the data in orderto discern patterns, trends, and correlations among variables.

Model Development: Construct a structural equation model (SEM) to depict the connections between client data privacy practises and occurrences of data breach incidents.

Model Validation: Employ diverse statistical tools to evaluate the Structural Equation Model (SEM) and determine its adequacy in terms of fit and predictive precision[10].

Expected Outcomes

The proposed methodology is anticipated to attain the following results:

Key elements Identification[11]: Determine the crucial elements that contribute to data breaches in the field of e-commerce.

Development of a Predictive Model[12]: Create a predictive algorithm to identify firms at a heightened risk of data breaches.

Enhanced Data Security Measures[13]: Offer guidance to firms on enhancing their data security protocols and mitigating the likelihood of data breaches.

The proposed technique offers a methodical way to comprehending the structural connectionsbetween client data privacy and data breaches in the field of e-commerce[14]. The results of this study can be utilised to enhance data security protocols and mitigate the likelihood of data breaches, hence yielding substantial advantages for both enterprises and customers.

Result analysies

To model and validate the structural relationship between client data privacy in e-commerce and data breaches, a simulation parameter table must be created[15].

Table 2: This table should take into account several crucial elements and characteristics. Hereis an illustration of what such a table could resemble:

Parameter	Description	Values/Type	Notes
1. Customer Data Types	E-commerce customer data types.	PII,Transactional	Important for understanding data
		Data, Browsing History	scope.
2. Data Privacy Measures	Protection of consumer data.	Encryption, Access Control, Data Anonymization	These measures affect data breach likelihood and
			severity.
3. E-Commerce Platform	E-commerce platform traits.	Platform (B2C, B2B) Platform Size -	Platforms vary in susceptibility.
Characteristics		Technology Used	
4. Data Breach Scenarios	Possible data breaches.	Hacking, Insider	Simulations of real- world breaches.
		Threat, Accidental Exposure	
5. Impact Assessment Metrics	Breach effect metrics.	Number of Affected Users, Financial	Data breach implications are quantified.
		Loss, Reputation	
		Damage	

6. Regulatory	Data protection	CCPA, GDPR, Local	Compliance affects
Compliance Factors	compliance.	Regulations	data privacy.
7. User Behavior Patterns	User behaviour on the platform.	Use frequency,	User behaviour can affect data breaches.
		transaction type, privacy settings	
8. Incident Response Strategies	Data breach responses.	Instant Notice Legal	Response
		Actions-Remediation Plans	effectiveness affects damage control.
9. Technology Adoption Rate	New e-commerce technology adoption frequency.	High-Medium-Low	Impacts security measure implementation
			speed.
10. Historical Data	E-commerce data	Frequency, severity,	Helps predict and
Breach Records	breach history.	affected data types	prepare for breaches.

This table is a conceptual framework and would need to be adjusted and populated withactual data for a specific e-commerce context[16]. The values/types column can be expanded or modified based on the specific requirements of the simulation model[17][18].

Table 3: a "Results Analysis" table for a study on "Modeling and Validating Structural Relationships among Customer Data Privacy in E-commerce and Data Breaches" involves presenting key findings in a structured format. Here's a template for such a table:

Variable	Description	Findings	Statistical Significance
Customer Data Privacy Concerns	Measures consumer data privacy concern.	High concern, especially in data-breach-prone sectors.	$p < 0.05$
E-commerce Data Handling Practices	Determines how e-commerce platforms safeguard client data.	Some platforms have strong security, some don't.	$p < 0.01$
Frequency of Data Breaches	Number of e-commerce data breaches.	A direct link between poor data handling and data breaches.	$p < 0.001$
Customer Trust in E-commerce	Assesses client data trust in e-commerceplatforms	Data breaches damage trust and raise privacy concerns.	$p < 0.05$
Regulatory Compliance	E-commerce platforms' data protection compliance.	Better compliancereduces data breachesand boosts customer trust.	$p < 0.01$
Impact on CustomerBehavior	Consumer behaviour changes due to dataprivacy concerns.	Data breaches and privacy concernslimit user interest and transaction frequency.	$p < 0.05$

The above table presents theoretical findings from a research study that examines the interconnections between client data privacy concerns, e-commerce[19][20] data handling practises, and the frequency of data breaches. The "Findings" column presents the main observations, while the "Statistical Significance" column offers a theoretical statistical metric (such as a p-value) to suggest the dependability of the observations.

Conclusion

In conclusion, today's digital marketplace requires modelling and validating the structural relationship between e-commerce customer data privacy and data breaches. Technological safeguards, regulatory compliance, customer awareness, and organisational policies complicate this interaction.This field's models show how e-commerce's poor data privacy practises increase data leaks. These breaches damage customer trust, loyalty, and corporate finances and legal standing. To reduce these threats, effective data privacy safeguards must beprioritised.Understanding privacy strategy effectiveness requires validating these models using empirical data and real-world case studies. This validation improves models to incorporate dynamic e-commerce ecosystems and cyber threats.Technologists, business executives, and policymakers must collaborate since customer data privacy and data breachesare linked. Comprehensive and proactive data privacy strategies can protect sensitive client data and e-commerce platforms.In conclusion, studying the structural relationship between client data privacy in e-commerce and data breaches is crucial for online business security and viability. In a digital environment, client data protection requires continuous study, model development, and collaboration.

References

[1].Surjandy, B. Vierena and C. Cassandra, "Analysis of Data Quality and Data Privacy Factors on the Factors of Intention to Buy and Decision to Buy on e-Commerce during Pandemic COVID-19," 2022 International Conference on InformationManagement and Technology (ICIMTech), Semarang, Indonesia, 2022, pp. 28-32, doi: 10.1109/ICIMTech55957.2022.9915182.

[2].G. Shejy and P. Chavan, "Sensitivity Support in Data Privacy Algorithms," 2022 2nd Asian Conference on Innovation in Technology (ASIANCON), Ravet, India, 2022, pp. 1-4, doi: 10.1109/ASIANCON55314.2022.9909096.

[3].S. Perumal, R. Aramugam, G. N. Samy, K. Krishnasamy and B. Shanmugam, "Proposed Customer's Sensitive Information Privacy Model for Financial Institution," 2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE), London, UK, 2019, pp. 203-207, doi: 10.1109/iCCECE46942.2019.8941918.

[4].Yidong Li, A. Yumeng, Huifang Li and Hairong Dong, "Anonymity-based data publishing for preserving customer privacy in railway systems," 2016 IEEE International Conference on Intelligent Rail Transportation (ICIRT), Birmingham, 2016, pp. 186-190, doi: 10.1109/ICIRT.2016.7588730.

[5].M. Wang, "Big Data Analysis and Mining Technology of Smart Grid Based on Privacy Protection," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2022, pp. 868-871, doi: 10.1109/ICCMC53470.2022.9753721.

[6].R. Pramanik and S. Prabhu, "Analysing Cyber Security and Data Privacy Models for Decision Making among Indian Consumers in an e-commerce environment," 2022 International Conference on Decision Aid Sciences and Applications (DASA), Chiangrai, Thailand, 2022, pp. 735-739, doi: 10.1109/DASA54658.2022.9765113.

[7].V. Suneetha, S. Suresh and V. Jhananie, "A Novel Framework using Apache Spark for Privacy Preservation of Healthcare Big Data," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 743-749, doi: 10.1109/ICIMIA48430.2020.9074867.

[8].Kaur, "A hybrid approach of privacy preserving data mining using suppression and perturbation techniques," 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bengaluru, India, 2017, pp. 306-311, doi: 10.1109/ICIMIA.2017.7975625.

[9].Parkavi, T. B. N. Shetty, S. G. Shibu, R. Ismail and R. A. Muthirakalayil, "Customer Feedback Analysis Based on Emotion Detection Using Machine Learning Techniques with Privacy Preservation," 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT), Kollam, India, 2023, pp. 1617-1624, doi: 10.1109/ICCPCT58313.2023.10244876.

[10]. Q. Zhao, Z. Ma, X. Hei, Y. Zhu and J. Niu, "A 3-D Structural Components Automatic Modeling Method Based on BIM," 2017 13th International Conference on Computational Intelligence and Security (CIS), Hong Kong, China, 2017, pp. 59-63, doi:

10.1109/CIS.2017.00021.

[11]. Y. T. Prasetyo and D. G. D. D. Fuente, "Determinant Factors Affecting Customer Satisfaction among Filipinos in Lazada Online Shopping during COVID-19Pandemic: A Structural Equation Modeling Approach," 2020 7th International Conference on Frontiers of Industrial Engineering (ICFIE), Singapore, 2020, pp. 48- 52, doi: 10.1109/ICFIE50845.2020.9266734.

[12]. S. Okamoto, H. Kojima, A. Yamagishi, K. Kato and A. Tamada, "Layered- Modeling of Affective and Sensory Experiences using Structural Equation Modeling: Touch Experiences of Plastic Surfaces as an Example," in IEEE Transactions on Affective Computing, vol. 12, no. 2, pp. 429-438, 1 April-June 2021, doi: 10.1109/TAFFC.2018.2879944.

[13]. H. C. R. Oliveira, S. Yanushkevich and M. Almekhlafi, "Sensitivity Analysis of Stroke Predictors Using Structural Equation Modeling and Bayesian Networks," 2022 IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB), Ottawa, ON, Canada, 2022, pp. 1-8, doi:10.1109/CIBCB55180.2022.9863028.

[14]. H. Nagano, S. Okamoto and Y. Yamada, "Modeling Semantically Multilayered Affective and Psychophysical Responses Toward Tactile Textures," in IEEE Transactions on Haptics, vol. 11, no. 4, pp. 568-578, 1 Oct.-Dec. 2018, doi: 10.1109/TOH.2018.2840703.

[15]. M. N. YAKUBU and M. KAH, "Nigerian Instructors' Acceptance of Learning Management Systems: A Structural Modeling Approach," 2020 IST-Africa Conference (IST-Africa), Kampala, Uganda, 2020, pp. 1-10.

[16]. O. G. Aguilar and A. Gutiérrez Aguilar, "A model validation to establish the relationship between teacher performance and student satisfaction," 2020 3rd International Conference of Inclusive Technology and Education (CONTIE), Baja California Sur, Mexico, 2020, pp. 202-207, doi: 10.1109/CONTIE51334.2020.00044.

[17]. Mukminin, A. Habibi, M. Muhaimin and L. D. Prasojo, "Exploring the DriversPredicting Behavioral Intention to Use m-Learning Management System: Partial Least Square Structural Equation Model," in IEEE Access, vol. 8, pp. 181356-181365,2020, doi: 10.1109/ACCESS.2020.3028474.

[18]. M. Taheri et al., "A Structural Equation Model Analysis of Computing Identity Sub-Constructs and Student Academic Persistence," 2018 IEEE Frontiers in Education Conference (FIE), San Jose, CA, USA, 2018, pp. 1-7, doi: 10.1109/FIE.2018.8658378.

[19]. Z. J. Belmonte, V. N. Jalbuna, J. Deligos and J. A. Viray, "Factors Affecting Customer Satisfaction among Filipinos in Online Grab Delivery during COVID-19 Pandemic: A Structural Equation Modeling Approach," 2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), Riga, Latvia, 2021, pp. 1-5, doi: 10.1109/ITMS52826.2021.9615282.

[20]. L. M. Guimarães and R. da Silva Lima, "Structural Modeling and Measuring Impact of Active Learning Methods in Engineering Education," in IEEE Transactions on Education, vol. 66, no. 6, pp. 543-552, Dec. 2023, doi: 10.1109/TE.2023.3259882.