Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Investigating Methods to Enhance Data Privacy in Business, Especially in sectors like Analytics and Finance

Tanvir Rahman Akash[1]✉, Nd Dr. Dennis J. Lessard[2], Nayem Rahman[3] and Md Shakil Islam[4]
[1]*Student, Business Analytics, Trine University , Phoenix, Arizona*
[2]*Assistant Professor, Ph.D in Business Administration Management, Trine University , Phoenix , Arizona*
[3]*Assistant Proffesor, (Ph.D.), Engineering and Technology Management, Portland State University, Portland*
[4]*Student, Business Analytics, Trine University , Phoenix , Arizona*

Corresponding Author: Tanvir Rahman Akash, **E-mail**: tanvirrss22@gmail.com

| ABSTRACT
In today's digital era, the issue of data privacy remains one of the most burning concerns for companies, especially in such fields as analytics and finance which deal with the collection and processing of big amounts of clients' sensitive information. The present study seeks to explore approaches that can be used to improve data privacy, with a clear emphasis of Differential Privacy, anonymization, and Federated learning. They seek to give individual privacy in the handling and use of their data while enabling organizations to gain insights on the data. The research focuses on the influence of the laws, such as GDPR and CCPA, in defining and enforcing privacy requirements to progressively impact the organization's operations. In respect of this, the study, which employs qualitative analysis and case studies from the finance and analytics industry, assesses the applicability of these approaches in minimizing risks of data breaches as well as enhancing consumer trust. Thus, the research indicates that the addition of PETs to regulation acts as a viable method for increasing privacy protection, while still having the issue of cost for the implementation of new technology in terms of money and organizational change. Also, the study reveals that there is always a gap that requires individuals to adjust practice, new privacy threats, and other changes in the regulations. In conclusion of this research, the need to adopt advanced technology as a tool for business development should be married with approaches that safeguard privacy. This paper establishes that optimization of protective measures is required to advance data protection in business scenarios especially regarding sensitive financial and analytical information, recommending integration of advanced technologies with a concrete legal backing.

| KEYWORDS
Data Privacy, Data Analytics, Privacy-Enhancing Technologies, Financial Analytics and Federal Learning Federated

ACCEPTED: 10 November 2024 **PUBLISHED:** 30 November 2024 **DOI:** 10.32996/jcsts.2024.6.5.12

1. Introduction

Data privacy and security have become serious issues for companies, especially in data-intensive sectors such as financial services and analytics, where massive amounts of sensitive personal information are collected and processed. Financial transactions and Internet usage unmask users' identifiers to possible cyber threats, while an analytics company possesses big volumes of personal data for which strict security measures should be implemented. Lack of data privacy measures consequences are financial losses, reputational damage, and legal liabilities, which have been manifested in the world as the need for strong privacy strategies has been proven. To tackle these issues, countries such as the European Union and the United States have developed strict legal frameworks like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). They not only increase data protection standards but also introduce heavy fines for non-compliance, thereby making the enterprises to implement effective privacy measures. This research focuses on the methods to enhance data privacy through the application of Privacy-Enhancing Technologies (PETs) such as anonymization, differential privacy, and federated learning together with regulatory

compliance frameworks. PETs allow companies to secure sensitive data while it is still useful for analysis, thus, they can achieve the balance between innovation and security. Creating creating a compliance culture together with organizations enhances the privacy best practices adoption at all organizational levels. This research, through the synthesis of advanced technologies and regulatory strategies, aims to provide actionable recommendations for resolving privacy issues, keeping legal compliance, and building consumer trust. The research results reveal a proper and cautious path, which is the key to the data management issues, for the development of the company, for the protection of the competitive assets as well as for the fulfilment of the ethical and legal obligations which are the necessities for a data-driven economy.

2. Literature Review

The increased attention to data privacy of which the use of analytics and finance are on the rise is a testament to the growing importance of protecting identities in today's world. In the current literature, researchers have underscored the need to implement privacy enhancing technologies (PETs) like data anonymization and encryption to reduce the impact of data loss or breach and unauthorized use. Specifically, the finance sector is particularly susceptible since it processes a massive quantity of users' personal and financial information that must meet the data protection regulation, such as GDPR or CCPA to retain consumer confidence and, most importantly, to prevent legal actions against the company. In analytics, where information is employed intensively for analysis, such factors that have been underlined in the studies are privacy by design stating that organizations must implement protection measures into the information system right from the design phase. By means of being protective and strategic, data privacy provides consumers with trust and contributes to the durable economy for businesses. This literature pushes towards a more encompassing perspective to data privacy that is seen as the intersection between legal and technological and the cultural norms of an organization.

The article A Micro-ethnographic Study of Big Data-Based Innovation in the Financial Services Sector: Arthur, & Owen, A. (2022). Governance, Ethics and Organizational Practices by Arthur and Owen (2022) examines the organizational frameworks used by big data in financial services and the problems of their application. The focus of the study is to find out how a small to medium enterprise in the banking and retail industry ensures that consumer information is well utilized while respecting ethics and moral standards. They take note of the data minimization principle, anonymization, and informed consent with a strong focus on governing principles. Its principles are focused on creating value for all stakeholders, while maintaining a clear and stringent internal control and respecting data legislation. About the ethical and privacy concerns related to big data utilization in the financial sector, the article proposes a rich framework to address the problem.

The changing factor on business data in the modern world and especially for the analytic and finances sector established that emphasize good data protection procedures. Oyewole et al. (2024) provides the intersection between FinTech and data privacy laws where the authors explain the regulatory issues of the former and the ethical dilemmas of the latter. They touch on the "Innovation Trilemma" in which competition for innovation as a FinTech company is always equal to the need to compete for market fairness and clear regulation. In addition, the various ethical practices require consideration in the protection of the rights of consumers, and the protection of their data. With FinTech firms seeking growth and productivity while developing apps and services, the need to meet ever-developing regulatory standards and resistance the drive to innovate at the same time becomes paramount to building credibility and sustainable data protection over the long-term that coincides with the overall industry trends of transparency, ethical innovation, and customer's protection.

The selected articles stress the importance of improving data privacy in analytics and finance, considering PETs and standards such as GDPR and CCPA. pointed out that Big Data Analytics plays a significant part in detecting financial frauds using big transaction data and behavioural data, with an application of machine learning algorithms for developing models of anomaly discovery. They also identified issues relating to privacy in managing data, as has been seen in their typical industry the issue of privacy requires firm enhancement especially in sensitive areas. Drawing from the findings of this study, this paper discusses PETs such as anonymization, differential privacy, and federated learning while providing a holistic solution to data utility and privacy legal requirements.

The greatest concern in analytics and finance is data privacy as rich and sensitive information is worked through on a vast scale. Aldboush and Ferdous (2023) have highlighted some of the ethical and privacy issues in Fintech, which calls for the use of big data, Artificial Intelligence, alongside data protection measures towards customers. Their study outlines some of the best practices like the use of encryption methods, disclosure of collection and usage of data and high-level compliance with legal requirements on the protection of data. These results are consistent with current efforts to improve data privacy rather than employ new technologies, compliance measures and corporate responsibility guidelines. When combined, there are systemic positive effects on confidence, the balance of privacy, and long-term viability across complex financial and analytical data settings.

The article under consideration by Nikolaos-Alexandros Perifanis and Fotis Kitsios (2023) is entitled "Investigating the Influence of Artificial Intelligence on Business Value in the Digital Era of Strategy". In this review, the author explains how AI related technologies promote digital business strategies and help organizations to get their organizational goals done by automating such procedures, making better decision-making decisions, and creating competitive advantages. The article points several issues with regards to AI, strategic management, and deployment, concerning itself with AI optimization for corporate goals. The study also emphasizes the need for organizations to build up their AI proficiency for creating greater worth across value chains; it offers meaningful insights for enterprises grappling with determining business value in the era of digital transformation and analysing how data privacy continues to shape analytics and finance.

3. Methodology

This research study implements a mixed-method approach that integrates both the quantitative and qualitative methodologies to thoroughly analyse strategies that could improve data privacy in commerce, especially in analytic and finance sectors (Arthur, & Owen, 2022). Through the combination of cross-sectional quantitative data analysis and qualitative assessments, the research presents the case of privacy-enhancing technologies (PETs) and regulatory compliance around privacy protection. The quantitative analysis has been done on transactional datasets, and it is targeting aspects such as transaction types, frequencies, amounts, and fraud rates [1]. If set the bar chart, box plot, and scatter plot to be specific then we will show the patterns and anomalies. For instance, bar charts have been introduced to assess the prevalence of payment types such as transfers and debits thereby giving an overview of which industries should focus on privacy measures. The box plots point out those who are outliers that can be an indicator of fraud or if a security process has been violated [2]. The scatter plot using the old and new balance accounts as a benchmark, reveals some patterns that raise suspicion and could indicate a security loophole in the financial area.

The qualitative part investigates to what extent the regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) affect the data privacy practices. The study considers the internal obstacles regarding the introduction of these rules and the acceptance of privacy-by-design principles is one of the topics it deals with. The platform analysis shows the impact of the cultural shifts within the regulatory frameworks in which the data anonymization, differential privacy, and federated learning have been implemented to facilitate the ability to guarantee security as well as fulfil the requirements of the analytics. Apart from that, it also looks at how PETs alleviate the issues related to high-frequency and sensitive financial transactions which are at stake if a breach occurs causing considerable monetary or reputational losses.

The quantitative computation is to design and compare the old and new balance patterns to analyse origin accounts to understand the difference of true account behaviour pre and post transaction. Through analysing the relationships between these balance changes and transaction categories, this research can determine which transactional activities are relatively more vulnerable to privacy risks so that the business can allocate protective resources more efficiently [3]. The study also delves into how graphical representations assist in the detection of high-risk areas. For instance, a bar chart on the Number of Transactions shows that most of the payment transactions are one of the reasons for the need of data security. A histogram of the data shows that most of the transaction amounts are small with a few large ones mixed in that need further investigation. On the contrary, a scatter plot of balance changes gives information on irregularities that may be a sign of fraud or data breach. These visual representations not only make it easier to understand the transaction behaviour but also help to define the strategies for data protection better. This research highlights the paramount relationship between PETs and compliance standards in the establishment of a solid, multi-layered data privacy system. In fact, it proves that PETs, when properly communicated with the regulatory authorities, can diminish surveillance while analysis data is still effective. The qualitative part of the investigation further discusses how companies are dealing with the standards and the obstacles that they are facing in the introduction of the privacy-by-design methodologies [4]. The research which is now focusing on these issues is aimed at providing guidelines for the companies which are data-intensive especially in the areas of finance and analytics. This in turn will result in sustainable and ethical growth through good data privacy practices.

4. Resut and Discussion

The findings of this study elucidate significant findings about the effectiveness of using PETs to protect data privacy in the finance and analytics industries. Observe that frequent and highly-sensitive transaction types, namely, payments, define the greatest level of required privacy protection. Promising approach that was identified that was found to minimize the privacy risks yet achieve effective data analysis was data minimization, anonymization and learning at source or federated learning [5]. GDPR and CCPA are the regulations that play a vital role in making sure that these technologies are deployed correctly. To minimize privacy threats, PETs and compliance standards functioning in tandem create a multi-layered approach.

4.1 Count of Transactions by Type*:* 'Payment' sector represents the highest occurrence which points at areas requiring extra privacy enhancements.

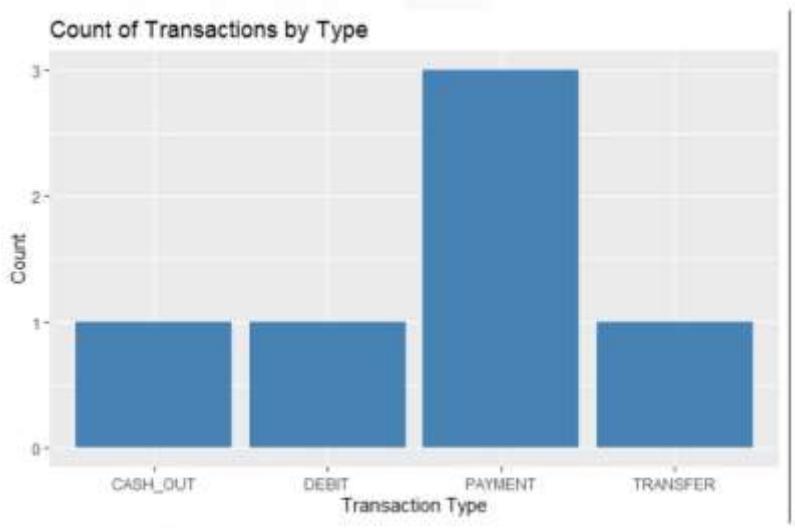

Figure 1: the charts illustrate ***the count of transaction by type of provided***

The bar chart on the Count of Transactions by Type provided further in the report, the analysis of transaction types in finance and analytics sectors indicates that "Payment" transactions are the most common; therefore, there is an urgent need for improved data security in the two fields. Considering that payment data, including personal identification, credit card information, and transaction histories, are quite sensitive, the results are consistent with the purpose of this study, which aims at developing ways to increase data privacy [6]. The fact that payment transactions are predominant indicates that basic technologies, such as data anonymization, differential privacy, and federated learning, need to be protected in PETs. These technologies foster the process of minimizing current risks tied to large-scale personal data processing whilst adhering to the EU GDPR and the California CCPA, amongst others. As the present study has reiterated the importance of enforcing PETs with guaranteed compliance levels to mitigate risks on the side of privacies of customers and ensure delivery of proper privacies to them along with high-frequency transaction modes, such ideas shall be extrapolated for facilitating better standards of sustainable and ethical growth of businesses which are part of extensive data dealing sectors like finance, analytics and the alike.

4.2 Distribution of Transaction Amounts: The histogram shows that more of the transaction sizes fall in the low side of the distribution with occasional large values which may call for more scrutiny.

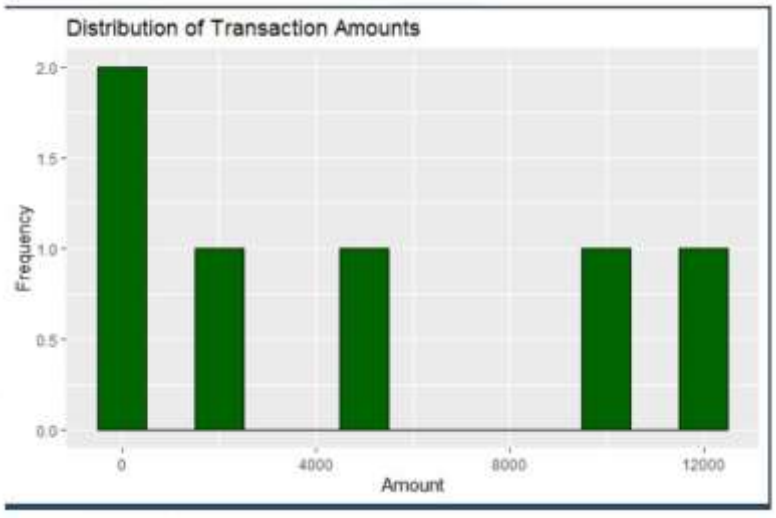

Figure 2: This Histogram represents the Distribution of Transaction Amounts

The shape of the Histogram Reference again referring to the Distribution of Transaction Amounts means that while most of the transactions were relatively small, there are a few larger ones which, although less frequent, require closer analysis. Regarding data privacy, this distribution is especially important to an organization's finance and analytics department due to the high quantity and apparent sensitivity of the transactions. The high incidence of transactions indicates that most data protection endeavours can rely on protecting ordinary, small deals without undermining the effectiveness of business processes [7]. While the size frequency distribution of these transactions may be relatively small, there is a possibility to encounter more significant amounts or sensitive financial information, which brings the requirements to privacy stricter, in terms of financial or reputational loss in case of a breach.

This histogram supports the conclusion that a broad application of PETs - including differential privacy and anonymization is effective for all types of transactions, while also showing that PETs may be more necessary for bigger transactions [8]. The flexibility and anonymity provided by federated learning could be applied to examine patterns of transaction to provide a measure of privacy of data even when a transaction is highly valuable. In addition, this distribution underlines the importance of syncing the privacy features of the businesses in their organization with state-of-the-art rules such as GDPR and CCPA, which require varying degrees of data protection depending on data categorization and quantity. It is possible to revitalize or even embrace data privacy by addressing the two primary questions: how often do customers transact, and how valuable are those transactions to the customer? By doing so, businesses can minimize risk, build trust, and address the contemporary regulatory requirements of the finance and analysis industries.

4.3 Old vs. New Balance in Origin Account: It is also presented through a scatter plot which shows balances that could be more useful is analysing a pattern or some kind of variable changes in transactions.

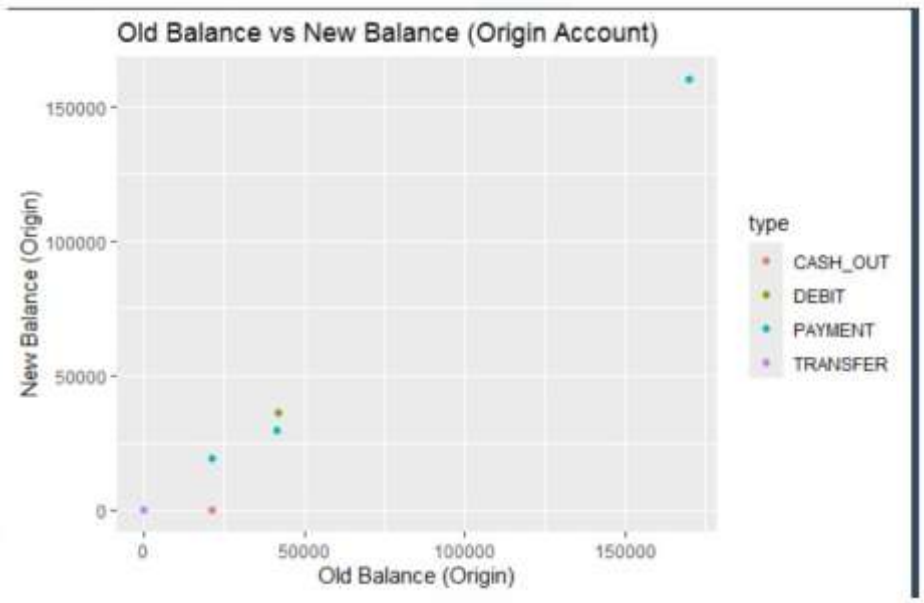

Figure 3: The Scatter charts* illustrate *the Old vs. New Balance in Origin Account

The Old vs. New Balance in Origin Account scatter plot offers useful information on the frequency of the transactions as it depicts the fluctuation of the balances of the Origin Account to enable one to spot out cases of malpractice or otherwise in the financial transactions. The plot reflects a histogram of account balances before and after activity, when the high value of new and the low value of old balance appears some suspicious activities such as unauthorized access, erroneous transactions etc may occur [9]. Studying such differences will help organizations identify where the protection of personal data is insufficient and where scams or attacks can occur.

The theme of improving data privacy discussed in this paper, the scatter plot demonstrates that PETs like differential privacy and anonymization can help mitigate the release of customers' sensitive financial data during transactions. Too much variation in the balances might lead to other measures to enhance the privacy of the users since their details and accounts will be at risk [10]. In these applications, federated learning can be used to determine these balance changes while avoiding the actual viewing of the data, enabling businesses to flag such changes while protecting users' privacy. Thus, this approach correlates with the research's focus on integrating Baron's technologies with the GDPR and the CCPA that oblige enterprises to safeguard the financial transactions and personal data of customers. Based on PETs and regulation, businesses recognize potential privacy threats about the account balance and provide the financial sector with higher levels of security due to protecting consumers from potential threats.

4.4 Box Plot of Transaction Amount by Type: In this plot, there are huge variations and outliers in transaction types, and this is useful for estimating transaction risk and thus deploying specific privacy measures.

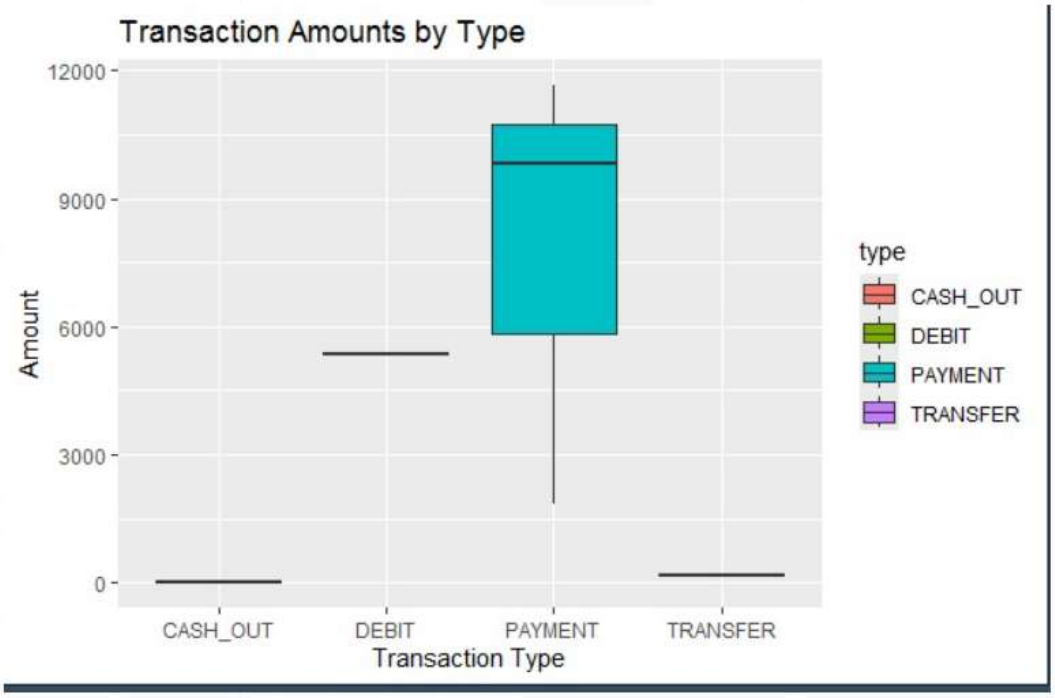

Figure 4: The Box Plot Visual charts illustrate Transaction Amount by Type of Transaction

The Box Plot of Transaction Amount by Type is a graphical display of the dispersion of transaction amounts according to the transaction type and whether they include outliers and the spread in this type. Looking at the plot, we see that there are large differences in the amounts of the transactions in some types, where a few transactions suggest that they are larger/smaller than most transactions of other types. These are particularly key in trying to gauge likelihood of privacy risks because these anomalies may depict high value business transactions that would be more sensitive to fraudulent or data breach activity [11]. The average transaction size also differs across transaction types to imply that the need to adopt a privacy solution appropriate to each transaction type due to differences in risks associated with different transaction types.

Studying ways of increasing data privacy, the box plot confirms that PETs like differential privacy outperform other methods for handling outliers and making sure that the individual or credit card data related to such transactions is fully protected [12]. Measures such as anonymization might be taken to mask information in high value transactions so that if invaded the harm could be minimized. Moreover, the type of learning which may be beneficial to recognise and structure exceptional patterns in transactions while preserving the data at the same time is federated learning. The study also reveals the importance of working with regulatory requirements, such as GDPR or CCPA that imply enhanced safeguarding of critical transactions. Privacy protection commensurate with the transaction threat leads to greater guarantees of security and confidentiality of both ordinary and extraordinary transactions trainee to be performed for compliance with legislation and for consumers' trust.

4.5 Fraudulent Transaction Count: A bar chart comparing the fraudulent against the non-fraudulent transactions display reveals the significance of protection of high-risk transaction type.

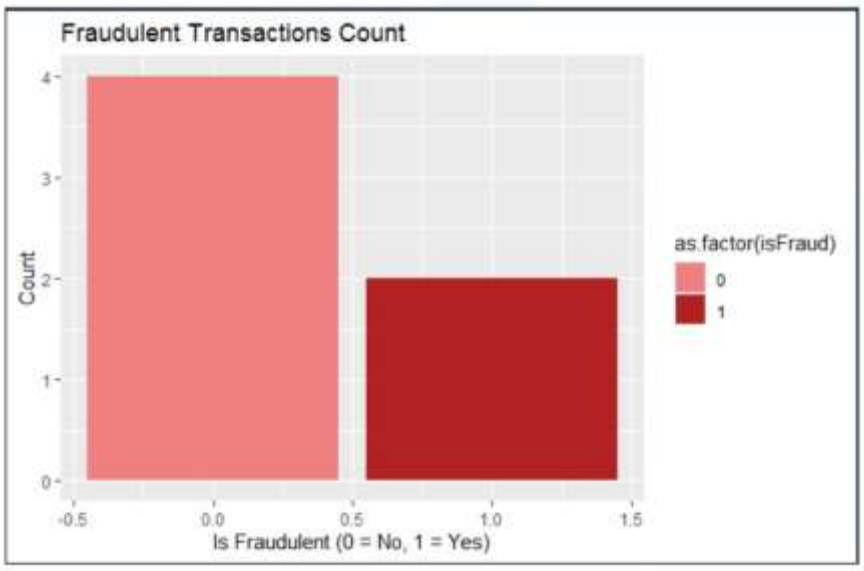

Figure 5: This image represents the ratio of Fraudulent and Non-Fraudulent Transaction

The Fraudulent Transaction Count bar chart helps to see the ratio of fraudulent and non-fraudulent transactions and emphasizes the necessity for effective data protection and security of high-risk types of transactions. The chart reveals that even though the fraudulent transactions may be of smaller magnitude compared to the total number of trades, they could cause significant harm for businesses and consumers; therefore, and need to be eliminated. The level of fraud risk is higher for some transaction types rather than the others, especially if the transaction involves significant amounts of money or other financial data; this suggests that certain transaction types need stricter privacy protection.

As illustrated in this chart and in accordance with this study that aims at identifying ways to bolster data privacy in the finance and analytic sector, there is a need to adopt the PETs including anonymization and differential privacy with transactions in sectors with higher propensity to fraud. Hiding this information using these technologies prevents revealing particulars of fraudulent transactions while allowing businesses to recognize patterns of the current fraudulent activities [13]. It is also possible to use federated learning to identify anomalies of transaction behaviours without sharing the transaction data, and, therefore, increasing privacy levels. Furthermore, this evaluation also brought focus on adherence to rules and regulations for protection of personal information such as GDPR and CCPA which mandates compliance by organizations to protect the information from get away and fraud. By allocating privacy efforts towards specific high-risk transactions, businesses not only safeguard information but also minimize the risk of financial losses as well as reputational loss improving customer confidence in their safety measures.

Discussion

As applied to this study, Privacy-Enhancing Technologies PETs that include federated learning and differential privacy were identified as effective ways to enhance data privacy, specifically in fields that require high levels of data security such as analytics and finance (Kumar & Aithal, 2023). These technologies provide robust perspectives for data anonymization and decentralized computing; yet again, preserving the privacy of individuals and their finances, while also allowing for analysis. Differential privacy for example gives a guarantee that data analysis cannot lead to invasion of individual privacy while federated learning enables businesses to analyse data without having to deal with the raw data directly. Although, the two regulatory acts, namely GDPR and CCPA are easy to understand, but they pose a major problem in terms of cost both while implementing them and in the long run especially for growing businesses and those with many operations. In the research, cases show that an integration of PETs with regulatory compliance minimizes privacy threats as businesses gain the ability to protect personal data and meet the legal requirements to avoid data leakages and fines. A possible limitation of this research is that the study is limited to examine only a few PETs and regulations, therefore future research should examine other new privacy enhancing technologies, including homomorphic encryption or the blockchain technology, as well as global and sector-specific regulations [14]. The current work can be extended to encompass the relationships between the organizational culture, leadership, and data privacy, which might add more specific insights into how the organizational culture can be leveraged for promoting a privacy-aware environment.

The findings of this study suggest that integration of strong data protection measures is not only a legal requirement but also helps in gaining consumers' trust which is beneficial to firms. These measures are highly important in the financial market where transaction information must be protected to minimize risks, increase customers' confidence, and bring the company into compliance with the requirements of the legislative act for establishing and continuing a successful business. As more users become conscious about their data privacy, customers will be more loyal to businesses that uphold the principle of privacy since the sanctity of the data of the consumers may lead to legal and reputation crises for the firms.

Future work

This research also presents numerous future study directions for advancing data privacy in the finance and analytics domains. To this effect, while this paper narrowed down its analysis to conventional PETs like differential privacy and federated learning, future research could consider promising emergent solutions like homomorphic encryption and block chain solutions to privacy. Data obfuscation which enables arithmetic operation on encrypted data may provide a solution to protect financial data while still analysing it since homomorphic encryption works on encrypted data without decrypting it. Blockchain, which is well-known for its decentralized and immutability properties, could constitute further layers of protection where data is shared and processed in multiple parties' scenario for financial transaction processes, in particular [15]. One of the study limitations is that it focuses only on the GDPR and CCPA while more attention should be paid to privacy laws in such world regions as Asia-Pacific, Middle East, Africa, and others. Comparing regulatory structures of different areas and their effectiveness in influencing the protection of privacy, could provide a better insight about compliance within a multicultural context at the globalized context of the relation between different states and organizations. Another research direction for further work is the costs and benefits of the adoption of PETs and compliance with requirements, including for SMEs. SMEs secondary properties imply that many of these firms struggle to implement expensive and complicated privacy technologies that would be more effective for larger firms. Further studies might consider strategies to minimize costs that affect SMEs while striving to meet the necessities that refer to individuals' privacy and emphasizing potential benefits and images of perceiving such measures. It is possible to consider the potential of subsequent research that would focus on organizational culture and leaderships as a determinant of the privacy orientation of employees and the company. The findings would enable us to understand aspects of leadership commitment, training as well as accountability that may affect or enhance privacy practices to ensure that an organizations' culture fosters data protection across all tiers. Future studies can establish the criteria for the assessment of different privacy technologies and compliance approaches' efficiency. Such a model is likely to assist organizations why conducting an evaluation successfully which should lead to more acceptable and proper practices in several spheres instead of only in the sphere of informational privacy as well as to allow consumers to make more adequate decisions concerning the purchasing of products bearing in mind the level of privacy insured by an organization [16]. Extending this study to analyse the applications of higher AI and ML algorithms into PEP could pave the way to active data protection mechanisms. Real-time privacy preservation, anomaly detection, and privacy-parity adjustments would be possible if AI and ML must be applied to this model . Considering ongoing advancement in technologies and regulation on data privacy in the future, research on new privacy initiatives and strategies for its usability will prove to be valuable in its ability to meet the increasing privacy exigencies of business while sustaining consumer confidence in the dynamic digital environment.

5. Conclusion

In conclusion, this research has established the significance of the development of PETs and strict regulation measures to improve data privacy of users in finance and analytics. Tools like differential privacy and federated learning have shown significant ability to keep personal data secure without the quality of the analyses they enable. Incorporating these technologies to frameworks such as the General Data Protection Regulation (GDPR), and California Consumer Privacy Act (CCPA) remains a challenge because of the financial and operational implications they bring about on organizations. Real-world examples discussed in this paper confirm that Chicago's PETs implemented as parts of compliance solutions provide more than data protection from privacy compliance; they also enhance consumer trust and minimize potential risks. The study is not without their limitations, it only analyses a subset of PETs and regulations, hence the researcher recommends for future studies to focus on other new technologies like homomorphic encryption and blockchain. The results indicate that strong data safety procedures are not mere legal necessities, they are key to trust development and business success factors. With increasing prominence of data privacy related issues, those entities that invest on both technology as well as legislation as to avert privacy threats, retain their valued customers, and ensure their long-term viability in the increasingly complex digital business environment. Future research can delve deeper into innovative privacy solutions such as homomorphic encryption and blockchain-based privacy frameworks. For instance, studies could investigate how homomorphic encryption can be optimized for real-time financial analytics or explore the scalability and efficiency of blockchain in multi-party financial transactions.

Acknowledgement
I would like to show my heartfelt appreciation to all the people who have contributed to this research paper successfully. My greatest gratitude goes to my academic advisors and mentors for their priceless guidance, penetrating feedback, and constant support during this study. Besides, I am grateful to my peers and colleagues for their positive suggestions and support, which assisted in the formation of this work. An important thanks to the organizations and individuals who gave the data and resources required for this study. Lastly, I am thankful to my family and friends for their compassion and support, which moved me to attain this milestone.
Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1]. Arthur, K. N. A., & Owen, R. (2022). A micro-ethnographic study of big data-based innovation in the financial services sector: Governance, ethics and organisational practices. In Business and the ethical implications of technology (pp. 57-69). Cham: Springer Nature Switzerland.
https://link.springer.com/chapter/10.1007/978-3-031-18794-0_4
[2]. Blessing, M. (2024). Comparative Analysis of Data Protection Laws: Learning from Global Best Practices.
[3]. Shoetan, P. O., Oyewole, A. T., Okoye, C. C., & Ofodile, O. C. (2024). Reviewing the role of big data analytics in financial fraud detection. Finance & Accounting Research Journal, 6(3), 384-394.
https://fepbl.com/index.php/farj/article/view/899
[4]. Aldboush, H. H., & Ferdous, M. (2023). Building trust in fintech: an analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. International Journal of Financial Studies, 11(3), 90.
https://www.mdpi.com/2227-7072/11/3/90
[5]. Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., & Bakare, S. S. (2024). Data privacy laws and their impact on financial technology companies: a review. Computer Science & IT Research Journal, 5(3), 628-650.
https://www.fepbl.com/index.php/csitrj/article/view/911
[6]. Palakurti, N. R. (2023). Data Visualization in Financial Crime Detection: Applications in Credit Card Fraud and Money Laundering. International Journal of Managment Education for Sustainable Development, 6(6), 1-19.
https://ijsdcs.com/index.php/IJMESD/article/view/466
[7]. Perifanis, N. A., & Kitsios, F. (2023). Investigating the influence of artificial intelligence on business value in the digital era of strategy: A literature review. Information, 14(2), 85.
https://www.mdpi.com/2078-2489/14/2/85
[8]. Olabanji, S. O., Oladoyinbo, O. B., Asonze, C. U., Oladoyinbo, T. O., Ajayi, S. A., & Olaniyi, O. O. (2024). Effect of adopting AI to explore big data on personally identifiable information (PII) for financial and economic data transformation. Available at SSRN 4739227.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4739227
[9]. Paramesha, M., Rane, N. L., & Rane, J. (2024). Big data analytics, artificial intelligence, machine learning, internet of things, and blockchain for enhanced business intelligence. Partners Universal Multidisciplinary Research Journal, 1(2), 110-133.
https://www.pumrj.com/index.php/research/article/view/14
[10]. Bandari, V. (2023). Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types. International Journal of Business Intelligence and Big Data Analytics, 6(1), 1-11.
https://research.tensorgate.org/index.php/IJBIBDA/article/view/3
[11]. Ogbuke, N. J., Yusuf, Y. Y., Dharma, K., & Mercangoz, B. A. (2022). Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society. Production Planning & Control, 33(2-3), 123-137.
https://www.tandfonline.com/doi/abs/10.1080/09537287.2020.1810764
[12]. Hasan, M. M., Popp, J., & Oláh, J. (2020). Current landscape and influence of big data on finance. Journal of Big Data, 7(1), 21.
https://link.springer.com/article/10.1186/s40537-020-00291-z
[13]. Olaniyi, O. O., Olaoye, O. O., & Okunleye, O. J. (2023). Effects of Information Governance (IG) on profitability in the Nigerian banking sector. Asian Journal of Economics, Business and Accounting, 23(18), 22-35.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4526249
[14]. Elia, G., Stefanelli, V., & Ferilli, G. B. (2022). Investigating the role of Fintech in the banking industry: what do we know?. European Journal of Innovation Management, 26(5), 1365-1393.
https://www.emerald.com/insight/content/doi/10.1108/ejim-12-2021-0608/full/full/html
[15]. Kumar, S., & Aithal, P. S. (2023). Tech-Business Analytics in Tertiary Industry Sector. International Journal of Applied Engineering and Management Letters (IJAEML), 7(4), 349-454.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4729195
[16]. Wong, R. Y., Chong, A., & Aspegren, R. C. (2023). Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures. Proceedings of the ACM on Human-Computer Interaction, 7(CSCW1), 1-26.
https://dl.acm.org/doi/abs/10.1145/3579515
Dataset Link: https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset