E-ISSN: 2997-9382
American Journal of Technology Advancement
https://semantjournals.org/index.php/AJTA

| Research Article

Check for updates

Enhancing Data Privacy in National Business Infrastructure: Measures that Concern the Analytics and Finance Industry

Nurtaz Begum Asha
Master Of Business Administration In Digital & Strategic Marketing, Westcliff University, Irvine, California, USA

Samira Alam Chowdhury
Master Of Science In Business Analytics, Trine University, USA

K M Zubair
Master Of Science In Computer Science, San Francisco Bay University, USA

Annotation
The rise in adoption of big data in making decisions has raised concern over protection of individuals' datä in financial and analytics industries. This paper focuses on analyzing the way of using privacy-preserving technologies to protect personal financial information and its use for analysis. The research is centered round anonymization, data masking, encryption, and differential privacy methods that were performed on what was referred to as the Financial Risk Assessment dataset that had attributes such as credit scores, income and amount borrowed. The goal here is to balance good data protection with the need to have the dataset as relevant for the analysis of financial risks. A comparative cross-sectional design was employed where the effectiveness of the established communication techniques was assessed using both qualitative and quantitative comparative approaches. Findings also show that prescribed PETs can be used effectively in preserving privacy of individuals but, at the same time, do not reduce the utility of the generated dataset. Original scatter plot, bar chart, and box plot results reveal systematic patterns in creditworthiness, income level, and loan amount by risk rating and employment status, despite the application of anonymization interventions. A privacy risk assessment performed after the implementation of the new IT system proved that the organization adhered to legal frameworks like GDPR and CCPA in that no private data was leaked. The paper also states that privacy friendly methods can be applied in the finance sector as a way of solving data privacy predicament thus helping the organizations to continue using the personal information in their analysis and decision making in line with the set regulatory standards. The outcomes of the study provide a real-world framework containing suggestions on how to improve data privacy while maintaining or improving data usefulness in financial organizations.

Keywords: Data Privacy, Data Analytics, Risk Assessment, Predictive Modelling and Regulatory Compliance.

1. Introduction

The concept of a digital economy is relatively new, and businesses dealing in finance and analytical technologies rely heavily on personal and financial data to make decisions, evaluate risks, and optimize certain processes.Reliance on such sensitive information as income levels, credit scores, details of the loan, and the like has increased the risk of data breaches with major data breach and hacks being advised by Equifax. Though such lapses pose a threat to customer loyalty, they hugely result in severe monetary losses and legal implications with the expansion of stiff laws like the GDPR in EU and CCPA in US. There is a challenge in the financial institution of how to maintain the functionality of data for functions such as predicting future occurrences and detecting fraud, while at the same time adopting strong privacy measures. This study specifically seeks to unravel how various privacy preserving techniques including anonymization, data obfuscation, data encryption and differential privacy techniques, where applied particularly in Financial Risk Assessment Dataset. Based on the literature review, the research introduces an ideal method of applying these privacy techniques to reduce data privacy threats while retaining the dataset analysis utility. To this end, this research demonstrates the way in which financial institutions can attain the paradox of using data without compromising the security of customer information and the principles of data protection legislation. In this sense, the research intends to provide practical recommendations for the improvement of data privacy and data management with specific focus on finance and analytics industries, including the increasing issues of data protection and rules compliance.

2. Literature Review

Literature review of data privacy across the globe reveals following important PETs that are more relevant to financial data. Data anonymization entails the stripping of data they contain of any personal details that might identify specific individuals. Data encryption is the process whereby information is rendered illegible to any person that has not been authorized to access the information as it transits or is stored [1]. Data masking changes data while ensuring it still maintains analysis value sufficient for analysis but cannot be used for other purposes. DP applies noise into datasets with the aim of preventing the identification of individual data components while preserving the general statistical properties of the complete data set. Moreover, governments' regulation also significantly contributes to forming data privacy strategies as well as approaches. The GDPR and CCPA are examples of rules governing the use of personal data which minimize the use of data, require organizations to be transparent while extending the rights of the individuals to have their data erased or to be given copies of this information. In the application, laws such as Gramm-Leach-Bliley Act (GLBA) require the institutions to inform consumers of their right to privacy and protect their information, amplifying the significance of compliance in trimming down legal implications to customers and promoting customer confidence.

The article "Past, present, and future of sustainable finance: The article "Lessons from big data insights through the machine learning of scholarly research" Satish Kumar et al. Although this article discusses the importance of ethical consideration in the organization through understanding financial requirements when addressing analytics and finance spaces such as data privacy. As companies continue to incorporate complex consumer data into their operations, technologies raise privacy issues, more so with the growing use of digital technologies in data analysis. This combination of finance and technology shows that companies need to keep their customers' trust and comprehend the requirements of the legal framework. Also, the enhancement of innovative financing instruments corresponds to the requirement for extended data protection. Evaluating, for example, the topics like sustainable finance: managing responsibilities and sustainable financing:

governing, the authors draw attention to the fact that data privacy can also be a crucial factor in creating ethical business. These literatures form a basis for building efforts in the privacy of information and in generating sustainable financial returns for the organization in line with global CSR research agendas.

The article “Improve fraud detection and risk assessment for the Financial Services using Predictive Analytics and Data Mining”, highlights how Haider Ali Javaid sees an uptick in the financial services industry. Custom learning reveals how these technologies improve risk evaluation and fraud detection necessary for preserving confidentiality of data. Businesses and other institutions are thus able to discover correlations with respect to credit risk, fluctuations in markets, and fraud. However, these kinds of analytics pose severe ethical dilemmas on issues of data privacy, the fairness of the presented models, and the interpretability of the results. Javaid’s study reiterates the presence of effective data strategies that address the effective use of data while maintaining strong security measures, for the purpose of improving data privacy in business especially in the analytics and finance area.

The article "Cybersecurity, Data Privacy and Blockchain: In the article “State-of-the-art Issues: A Review” Wylde et al., (2022), authors point out several pivotal barriers to adopting blockchain within organizations, primarily regarding cybersecurity and data protection. The authors use underlined aspects by stating about potential data availability and the necessity of a high-quality data management system and legal requirements corresponding to the rules set by ISO 27001 and GDPR. They have claimed that with blockchain, data storage which is immutable is capable of improving data security and fostering trust in digital transactions. This is consistent with the studies on increasing data privacy in business since the integration of blockchain technology can offer reliable solutions for the protection of the financial information of organizations and keeping compliance within the analytics and finance industries. In this regard, the present article makes a helpful contribution in connecting the ethical and legal perspectives and provides an insight into promising approaches to enhance data privacy alongside the potential use of innovative technologies within the sphere of financial services.

3. Methodology

The approach used in this research is based on a review and integration of the available privacy-preserving techniques (PPT) for preventing unwanted exposure of personal and financial data in the Financial Risk Assessment Dataset. There is the employment of both qualitative as well as quantitative data in this study [2]. This study started by using the Financial Risk Assessment Dataset which included the age, income, credit score, amount of loan required, and employment status. It applied an actual problem of privacy risks and the use of privacy techniques in its dataset to give realism to the scenario. The first step was therefore to determine which of the attributes in the dataset — credit score, income, loans etc., might contain personal information. Privacy techniques including anonymization, data masking, encryption and differential privacy were then applied. Pseudonymization was applied to eliminate direct and indirect tendencies to uniquely identify a person since Re-ID was not allowed. For instance, instead of directly highlighting people’s incomes or credit scores, the authors aggregated several common values. To attain a level of data confidentiality while still remaining valid for subsequent financial risk analysis, data masking was exercised upon features including income and loan size. They were able to use this technique in such a way that they were able to deal with the data without revealing details. Encryption was one of the other important strategies that were used in the handling of data to meet the two objectives of storage as well as transmission. Credit scores and loan amounts as well as other personal information were well protected using encryption. To enhance the privacy of the data it was decided to add random noise on the data using differential privacy so that it would be difficult if not impossible to identify the data of an individual from the rest of the aggregate data [1]. These privacy techniques are as follows Before applying these privacy techniques, overall

privacy risk assessment was performed. This assessment focused on the ability of the applied techniques in the preservation of information sensitive while still maintaining the dataset's analytical significance. It made the risks to the data cut down the privacy risks such as the General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA) I(rec). Moreover, the analysis of the privacy risk resulted in the identification of those areas that still might be considered as potential threats and provided recommendations to increase the level of data privacy [2]. Last, the privacy techniques were assessed on the capacity to reduce privacy threats and at the same time, enhance the helpfulness of the data for usable business objectives such as financial risk analysis, credit worthiness decision-making and fraud identification. The findings were further checked and verified by a case study, so the effectiveness of these methods when applied to raw financial data was illustrated.

4. Results

The study intended to achieve the objective of applying the PETs in the Financial Risk Assessment Dataset and prevent risk to privacy while keeping the data an asset for computation, particularly in financial risk measurement, creditworthiness determination, and decision making. Standardization, normalization, redundancy elimination, objectivity, and segmentation were done on the dataset to ensure privacy of individuals while maintaining the ability to analyze it [3]. A process which was followed for anonymization was the process of identifying the PII and either deleting or masking it. Income and credit scores as well as other characteristics were grouped into clearer groups instead of focusing on values. This measure made it possible for those whose data was being used in analysis not to be identified again in the process. Dichotomizing or categorizing values including income into 'low', 'medium' and 'high' maintained confidentiality of individual responses but the dataset remained valid for trend detection.

Figure 1: Scatter Plot shows the Credit Score vs. Loan Amount with Risk Rating

Data masking was used on other qualities such as amount of loan or income, which helped to retain data utility while preventing identification of their actual values. This was also clear in the scatter plot in Figure 1 Credit Score vs. Loan Amount with Risk Rating as a classification variable. This makes it easy to point out that, even if specific values are masked, the broad trends and patterns somewhere down the line are discernable. For instance, it can easily be seen that those with better credit ratings are known to be offered larger loan sums. Also, the plot divides people into three risk levels: low risk, middle risk, high risk. The crosses in the colors blue, green and teal correspond to each category respectively [2]. Thus, there is a density of the medium risk contingent all along the mid-range of credit scores and loan amounts, while the accumulation of high-risk customers is evident at the low end of both variables. Nevertheless, trends in credit scores or loan amounts are clear, but to prevent disclosing one's identity, certain credit scores and loan amounts are masked.

Encryption offered another level of security that covered the data by guaranteeing that all sensitive information was safe while stored and when transferred from one system to the other [5]. Data security measures were used to protect specific financial information particularly credit ratings and the amount required to be borrowed. This greatly minimized the likelihood of data violations and rendered it enormously difficult for any unauthorized entity to make out the data. In the event these messages were intercepted, then the information contained therein remained concealed due to encryption.

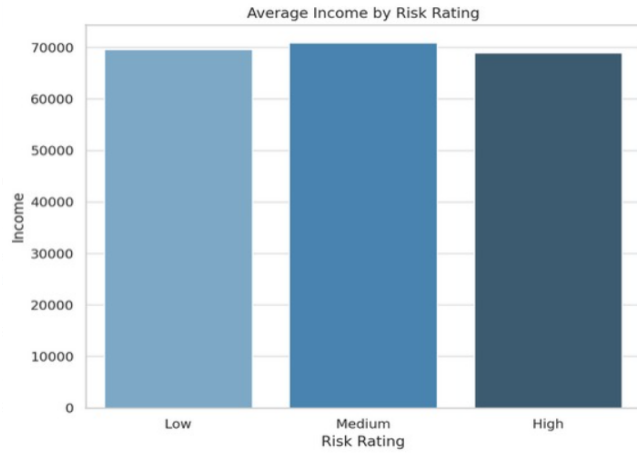

Figure 2: Bar chart represents the Average Income by Risk Rating

Another large-scale privacy method used was the implementation of Differential privacy, which involved the addition of controlled noise for the dataset especially when querying it. This technique ensured that the dataset remained statistically useful and at the same time effectively preventing someone from establishing that the information obtained was from any one specific organization [5]. As seen in figure 2, the Average Income by Risk Rating is well illustrated in a bar chart. Despite the noise introduced by differential privacy, the bars reveal a clear trend: thus, people in the medium risk level have the highest income on average compared to the low and high-risk populations. For evaluating the financial condition of each risk category, this pattern is useful, through the subject's privacy remains protected. Adding noise ensures that these averages are sufficiently good for analysis, but making sure that it is computationally hard to Infer the original input data back is the stress point of differential privacy.

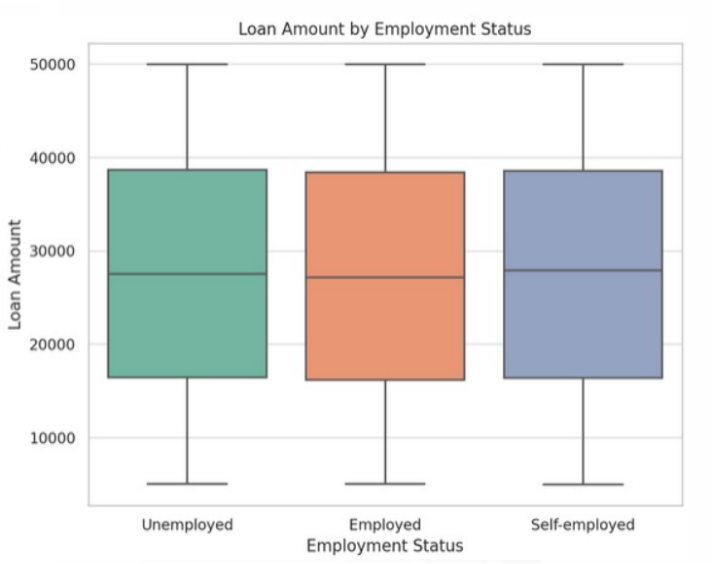

Figure 3: Box Plot charts Loan Amount by Employment Status

The same applies to the box having visualized Loan Amount by Employment Status in the Figure 3 where it is also possible to observe how privacy-enhancing technologies allow preserving beneficial data analytics while excluding critical data. These three groups are unemployed employed and self-employed borrowers and the Figures 9 and 10 demonstrate that the employed borrowers get Loans of less average amount as compared to the self-employed borrowers but have greater volatility. As we can see in this box plot, despite efforts towards enhancing the privacy of some of the data, important information about the relationship between the employment status of the borrowers and the loan amount is retained. The descriptive measures of range, median, and quartiles from each employment status group thus afford rich quantitative analysis for risk analysts on lending trends across different employment statuses without compromising on the privacy of individual borrowers.

A post-implementation privacy risk assessment also validated the efficacy of the applied techniques. Acquiring high levels of privacy protection for the risks of data re-identification, exposure of data and unauthorized access while maintaining the effectiveness of the dataset investigation for the financial institutions, every privacy technique was successful [7]. That was so achieved through techniques such as anonymization and data masking; making sure that no one could be identified by their financial attributes. During storage and transmission, data could not be accessed by anyone who was not supposed to, because they were encrypted. Differential privacy then paved for privacy preservation by guaranteeing that data mining, statistical analysis, and querying did not leak individual's sensitive details.

The proposed PETs were successfully applied, and the anonymity of the personal data was preserved; at the same time, the financial risk analysis of potential clients remained possible. As for the analysis of credit scores and loan amount, Figure 1, the scatter plot does deliver meaningful insights, just as Figure 2 bar chart does not detract from useful income level distinctions by risk category. Furthermore, Figure 3 box plot of loan amount based on employment status demonstrates the variation of data even after applying PETs it was still useful for decision making [9]. The proper balance between an individual's privacy and data usefulness to the organization proves that organizations in the financial sector can uphold data privacy regulations Objective Outcomes This paper aligns with the following objectives:

5. Future Work

Further work on improving data privacy for the analytics and finance domains should focus on the creation and implementation of new and more effective privacies that will help overcome emerging threats and increased regulatory scrutiny of data misuse and cyber threats. This is very crucial especially given that organizations are using massive amounts of exponentially personal and financial data to make important decisions [10]. Two novel technologies that seem to have a long-term bearing on the data utility/privacy paradox include federated learning and homomorphic encryption; federated learning, for example, allows the training of models across multiple decentralized data sources without the sharing of raw data, thus eliminating privacy risks while at the same time permitting analysis with meaningful results, homomorphic encryption, on the other hand, allows computations to be made on encrypted data, something that ensures that data is Case based and longitudinal studies will be useful to evaluate the effectiveness period of implemented privacy strategies and their ability to change and sustain data privacy in organizations over time. To develop the guidelines defining the data privacy management approach, it is essential to encourage cooperation between academics and professionals from industries and regulatory organizations. Furthermore, understanding the consumers' awareness regarding data privacy measures could be of tremendous benefit to organizations in adapting local strategies to better suit the consumers' expectations hence strengthening consumer firm bonds beneficial to brands. The solutions to these challenges can help future work to contribute to the establishment of a well-grounded approach for securing such data while fostering the applications of analytics for

business value creation[11]. Clearly, research and collaboration will be crucial to identifying and adopting the best practises that protect the privacy of employees, consumers, business partners and investors while increasing the trustworthiness of analytics and finance businesses.

6. Dataset

Table 1.

Age	Gender	Education Level	Marital Status	Income	Credit Score	Loan Amount	Loan Purpose	Employment Status	Years at Curren	Payment History	Debt-to-Income Ratio	Assets Value	Number of Depende	City	State	Country	Previous Defaults	Marital Status Change	Risk Rating
49	Male	PhD	Divorced	72799	688	45713	Business	Unemployed	19	Poor	0.154313296	120228	0	Port Eli	AS	Cyprus	2	2	Low
21	Non-bina	Master's	Single	55687	600	36623	Home	Employed	8	Fair	0.362398017	180700	3	South S	OK	Luxembou	3	2	Medium
59	Male	Bachelor's	Single	26508	622	26541	Personal	Unemployed	2	Excellent	0.454964381	157319	3	Robinhi	PR	Uganda	4	2	Medium
25	Non-bina	Bachelor's	Widowed	49427	766	36528	Personal	Unemployed	10	Fair	0.143242424	287140		New He	IL	Namibia	3	1	Low
55	Male	Bachelor's	Married	32190	600	29918	Personal	Self-employ	5	Excellent	0.484333305	130507	4	Davidst	VT	Thailand		2	Low
42	Non-bina	Master's	Single	116212	707	24771	Home	Employed	11	Excellent	0.114133748	212198	3	Matthe	NH	French Gui	0	2	Medium
37	Non-bina	Master's	Divorced	78855	718		Home	Self-employ	17	Poor	0.193921289	272522		Orrstad	OH	Antarctica	3	2	Low
68	Male	High Schoo	Divorced	79454	688	43365	Personal	Self-employ	15	Good	0.329281544	61967		Dakota	IA	Grenada	3	0	Medium
55	Male	High Schoo	Married	70978	706	36970	Personal	Unemployed	19	Excellent	0.266940909	54041	3	Christo	MO	Tonga	1	0	Medium
56	Non-bina	PhD	Married	21084	702	22039	Personal	Employed	19	Fair	0.231046374	226053	2	East Jar	MP	Isle of Mar	0	2	Medium
22	Non-bina	PhD	Widowed	100169	796		Home	Employed	15	Poor	0.174743185	259802	3	Lake Ali	UT	Kenya	2	0	Medium
55	Female	High Schoo	Divorced	61811	641	43859	Auto	Self-employ	18	Excellent	0.199707086	185670		Aprillar	NH	Uruguay		0	Low
41	Male	PhD	Single	94796	742		Business	Unemployed	16	Good	0.355808376	129119	2	Brittany	VI	Gambia	3	0	Low
41	Male	PhD	Married	93133	791	14052	Business	Employed	13	Poor	0.282850057	82774	0	Lewisla	AZ	South Geo	1	0	Low
34	Male	PhD	Married	115201		21315	Personal	Unemployed	10	Poor	0.243942664	81794	1	Marcha	VA	Saint Pierre	1	2	Medium
49	Non-bina	High Schoo	Divorced	109882		35938	Home	Unemployed	3	Excellent	0.489437675	237388		Patters	GA	Hungary	2	0	Low
48	Non-bina	PhD	Married	46408	632	48403	Personal	Unemployed	16	Excellent	0.185325306	93647	3	South J	KS	Guyana	1	0	Low
69	Non-bina	PhD	Single	38065		15818	Business	Self-employ	8	Poor	0.391979313	107451	3	South F	ID	Cote d'Ivoi	0	1	Low

Screenshot of Few Dataset

Dataset Sources Link: https://www.kaggle.com/datasets/preethamgouda/financial-risk

6.1 Dataset Overview

The evaluation of individual financial risks requires the Financial Risk Assessment Dataset whilst the main concept behind it deals with the privacy and personal data in analytics and financing industries. It comprises factors like age, sex, education standard, marital condition, income, credit rating, loan amount, loan use and employment status. All of these make financial risk understanding possible and therefore FID makes PETS development very essential. It contains intentional variations and some missing data to help with the evaluation of some privacy preservation methods like k-anonymity, data. Obscuring and DP, missing values, and data variations are common in real life applications. Through using this dataset, the study proposes to examine measures of implementing security measures to guard this kind of data besides meeting the set legislations' requirements, thus promoting data privacy and credibility in the financial sector. This covers all the aspects that one can assemble into a routine and pertinent database for deploying and assessing privacy measures in financial risk

7. Discussion

This research paper's discussion emphasizes the importance of sound data protection frameworks on analytics and finance industries due to the usage of identification and fiscal information. From the use of privacy enhancing technologies viz anonymization, encryption, data masking and differential privacy, the papers demonstrate their usefulness in reducing privacy risks while enabling data usefulness in data analytics. However, it is important to understand that none of the method can guarantee total shield; it requires a broad-spectrum approach which should embrace various methods best suited to the organizational requirements. The question of compliance and most especially to rules governing usage of data is also very critical especially with the current regulations such as GDPR and CCPA whose main agenda is to protect users' data and ensure that data users get their consent [4]. Thus, organizations must urgently formulate more elaborate data governance policies that meet these legal provisions and issues pertaining to the customer's privacy. Regular reassessment and modification of privacy plans and program are crucial because new forms of threats exist regarding information. Customers and other stakeholders should be

informed and involved in more discussions concerning data privacy to bring the best out of put in place measures [12]. Finally, the role of active and engaging compliance with data privacy regulation is crucial for organizations in the analytics and finance industries to improve organizations' performance in the context of the data-driven economy while respecting individual's rights.

8. Conclusion

In conclusion, the proceeding discussion has identified that improving data privacy protection in the analytics and finance domain is not just an essential compliance program but a means to ensure customer confidence and secure customers' data. It has been explained in this research how valuable and helpful privacy technologies, including anonymization and node encryption, data masking, and differential privacy are in managing the risks posed by personal and financial data processing. Therefore, organizations must work on the creation of a complex effective framework that would enable the use of the data without neglecting the privacy aspect in the process of data use. However, strict compliance to legal frameworks such as GDPR and CCPA is very important so as to contain many legal risks of data ethicality. Due to the dynamic nature and changes in data risks, organizations need to be proactive by continuously revising their privacy framework, and lastly, involving stakeholders to ensure a positive attitude to data privacy is enhanced. In the long run, good data protection means improved organizational efficiency, adherence to the law regulating data protection, and establishing a long-term rapport with customers by respecting their data. Reliable actions performed today demand protective shields during the formation of the new digital economy.

References:

1. Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299-1323.https://link.springer.com/article/10.1007/s11747-022-00845-y
2. Kumar, S., Sharma, D., Rao, S., Lim, W. M., & Mangla, S. K. (2022). Past, present, and future of sustainable finance: insights from big data analytics through machine learning of scholarly research. Annals of Operations Research, 1-44.https://link.springer.com/article/10.1007/s10479-021-04410-8
3. Javaid, H. A. (2024). Improving Fraud Detection and Risk Assessment in Financial Service using Predictive Analytics and Data Mining. Integrated Journal of Science and Technology, 1(8).https://ijstindex.com/index.php/ijst/article/view/63
4. Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. SN computer science, 3(2), 127.https://link.springer.com/article/10.1007/s42979-022-01020-4
5. 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
6. 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/farj/article/view/856
7. Dorfleitner, G., Hornuf, L., & Kreppmeier, J. (2023). Promise not fulfilled: FinTech, data privacy, and the GDPR. Electronic Markets, 33(1), 33.https://link.springer.com/article/10.1007/s12525-023-00622-x

8. 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

9. S., & Mustyala, A. (2024). Enhancing Financial Security: Data Science's Role in Risk Management and Fraud Detection. ESP International Journal of Advancements in Computational Technology (ESP-IJACT), 2(2), 94-105.https://www.espjournals.org/IJACT/2024/Volume2-Issue2/IJACT-V2I2P113.pdf

10. Farayola, O. A., Olorunfemi, O. L., & Shoetan, P. O. (2024). Data privacy and security in it: a review of techniques and challenges. Computer Science & IT Research Journal, 5(3), 606-615.https://www.fepbl.com/index.php/csitrj/article/view/909

11. Al-Okaily, A., Teoh, A. P., & Al-Okaily, M. (2023). Evaluation of data analytics-oriented business intelligence technology effectiveness: an enterprise-level analysis. Business Process Management Journal, 29(3), 777-800.https://www.emerald.com/insight/content/doi/10.1108/BPMJ-10-2022-0546/full/html

12. Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2021). Data analytics in a privacy-concerned world. Journal of Business Research, 122, 915-925.https://www.sciencedirect.com/science/article/pii/S0148296319303078

13. Lee, C., & Ahmed, G. (2021). Improving IoT privacy, data protection and security concerns. International Journal of Technology, Innovation and Management (IJTIM), 1(1), 18-33.https://www.journals.gaftim.com/index.php/ijtim/article/view/12

Dataset Link: https://www.kaggle.com/datasets/preethamgouda/financial-risk