Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 08 Issue 01
2024

Research Article
https://doi.org/10.56979/801/2024

Analyzing the Impact of Cybercrime and Its Security in Banking Sectors of Pakistan by Using Data Mining

Afsheen Riaz[1], Sadaqat Ali Ramay[1], Farwa Abbas[1], Asif Hussain[1], Nabgha Naveed[1], and Tahir Abbas[1]

[1]Department of Computer Science, Faculty of Science and Technology, TIMES Institute, Multan, Pakistan.
*Corresponding Author: Sadaqat Ali. Email: drsadaqatali@t.edu.pk

Received: August 11, 2024 **Accepted**: October 15, 2024

Abstract: With the rapid digitization of banking services, present day financial institutions are facing threats from cybercriminals. Traditional methods of fraud detection have established inadequate against cyber threats, prompting the adoption of superior technology inclusive of records mining techniques. In this study, we explored the impact of cybercrime on the banking sector in Pakistan by employing data mining techniques. Our dataset consists of a wide range of variables, from cybercrime types and financial losses to customer trust and regulatory compliance. Utilizing classification models, Random Forest with 94% accuracy, Support Vector Machine (SVM) with 93% accuracy, and Decision Tree with 92% accuracy. This research highlights the need for strong security measures in banks to tackle cyber threats. Policymakers and bank professionals can use our findings to make banking safer. Financial institutions can protect their assets and customer information by using fraud detection techniques, thereby increasing trust and confidence in the system in digital banking.

Keywords: Cybercrime; Banking Sector; Security; Data Mining; Classification Models; Random Forest; Decision Tree; Support Vector Machine (SVM).

1. Introduction

In the digital age, the threat of cybercrime become a significant concern, impacting critical areas such as privacy, national security, societal norms, and intellectual property rights. By the advancements in technology, the banking growth increases day by day. However, with this growth, the risks associated with banking security have also increased [1]

Cybercrime is become a serious threat for the banking industry. The digital platforms become more advance, cybercriminals have increased and gain access to Pakistani banks, this activity leading to unauthorized access, fraud, and disruptions in banking operations [3].

Data mining techniques are used to detect unknown patterns in data. In the banking industry, machine learning and data mining methods becomes popular methods for detecting cybercrime. It analyzes large datasets to identify patterns that indicate fraudulent behavior, such as phishing attempts, malware, and fraudulent transactions. When the banking industry is compromised by cyberattacks [4].

A bank's profitability and stability can be adversely affected by fraud losses, such as unauthorized transfers. The banking sector in Pakistan faces growing cybersecurity threats due to the increasing prevalence of cybercrime. By analyzing cyber threats and their implications, banks can implement proactive security measures to mitigate risks and enhance resilience.

The study utilizes data mining techniques, such as Random Forest (RF), Decision Tree (DT), and Support Vector Machine (SVM) algorithms, to analyze banking sector data. Cyberattacks may damage a company's reputation, leading to the loss of customers. Cyberattacks could undermine the financial ecosystem of Pakistan, damaging banks in a wide range of ways. Pakistani banks are adopting various security measures to protect their systems, infrastructure, and customer information in light of the increasing cybercrime threat. Among the measures are firewalls, encryption, multifactor authentication, intrusion detection systems, and continuous employee training. Because cyber threats are rapidly evolving, a proactive approach to cybersecurity is required, which requires continuous evaluation of their effectiveness [4].

This study examines the security measures taken by Pakistani banks in order to mitigate cyber risks, assessing their strengths and weaknesses to assess their effectiveness and identify areas for improvement. Data mining techniques will also be used to analyze large amounts of data gathered from banks, cybersecurity reports, and other relevant sources. Using this analysis, meaningful patterns, trends, and vulnerabilities related to cybercrime in Pakistan's banking sector will be identified. A comprehensive understanding of cybercrime and the effectiveness of security measures is crucial for the banking sector. When developing robust security strategies tailored to the unique challenges faced by Pakistani banks, banking professionals will benefit from the findings of this study. By applying the insights gained, policymakers and regulators can improve the resilience and security of the financial system. By investigating how cybercrime affects banking, furthering cybersecurity, and enriching future research, researchers and academicians can contribute to the current understanding of cybercrime [5].

2. Literature Review

This study uses research and statistical analysis to evaluate the role of cybersecurity in preventing unauthorized access and data leakage in Jordanian banks using SPSS tools. Relative importance index (RII) was used to analyze the significance of different statements and tests [6].

About 81.5% of the sample also agreed that banks with cybersecurity can provide a secure platform for digital financial services and thus increase their competitive advantage due to being ranked first in the category and overall ranking (RII = 0.754). Research I investigated the impact of cybercrime on the banking sector and the security of the Pakistani banking system using data mining and machine learning. The research conducted in this article focuses on the impact of cybersecurity on the prevention and reduction of electronic crime in the Jordanian financial sector. However, the main difference in their research is that there is no specific focus on the types and consequences of cybercrimes in the banking sector. This study did not use advanced data mining or machine learning techniques to analyze the data collected from the survey [7].

In their systematic analysis, [8] examine the usage of biometric systems to enhance cyber security of banking sector. They highlight the growing popularity of biometric authentication across various sectors and emphasize its reliability in verifying individuals based on physical attributes and behavioral traits.

Through a systematic literature review, [9] identify key features of biometric systems in conventional and Islamic banking, aiming to provide enhanced safety and security to the banking industry. The study does not explore the potential application of predictive analytics techniques to predict and prevent cyber security threats in the banking sector. [10] research does not include a comparative analysis of different machine learning algorithms for detecting and mitigating cyber security threats in the banking sector. The author [10] looked into finding online crimes using computer programs. They used tools like SVM, KNN, and got 91% and 79.56% correct results with SVM and KNN. The study by [10] study didn't focus specifically on the banking sector. This general approach might miss important details and challenges unique to banking cyber threats. Additionally, their research didn't explore the effectiveness of tools like Random Forest and Decision Tree.

A study entitled "Big Data Applications in the Banking Sector: In "A Bibliometric Analysis Approach" by Haitham Nobanee, Mehroz Nida Dilshad, Saeed Al Shamsi, and three others provides an overview of the literature on big data applications in banking. A number of themes emerged from the reviewed studies, including investment, profit, competition, credit risk analysis, banking crime, and fintech. A detailed analysis and discussion of these themes is provided within the report. In the review, big data is underscored as an important and valuable tool for the banking and financial industries. Furthermore, the authors suggest areas for further research and development in big data analytics in the banking industry. According to them, big data analytics can enhance customer experiences and optimize business operations

The Following Table represent the results of previous research

Table 1. Literature Review Previous Author Work.

Author	Topic	Key Contribution	Research Gap
Amer el Al,	Role of cyber security in preventing unauthorized access and data breaches in Jordanian banks	Surveys, Statistical Analysis, SPSS Tool	Lack of focus on types and prevalence of electronic crimes; no use of advanced data mining or machine learning techniques
Khan et al	usage of biometric systems to enhance cyber security in the banking sector	Highlighted biometric system to enhance security features in banking sectors	No exploration of predictive analytics for cybersecurity threats; Absence of comparative analysis of machine learning algorithms for threat detection in banking
Duc M Cao et al	online crimes using computer programs	Focus on online crimes and used Computer Programs, SVM, KNN	Lack of focus on banking sector; Did not explore Random Forest and Decision Tree effectiveness
(Nobanee *et al.*, 2021	Big Data Applications in the Banking Sector: In "A Bibliometric Analysis Approach	Use of Big data for banking sector including investment, profit, competition, credit risk analysis, banking crime.	Specific impact within banking themes; future R&D in big data analytics

3. Methodology

Data mining techniques are used to extract insights and patterns from large datasets related to cybercrime incidents, security measures, and vulnerabilities in the banking industry. In response to these insights, the banking industry developed cybercrime risk reduction strategies. By analyzing cybercrime incidents using machine learning and data mining techniques, this study developed more effective security measures and gained a deeper understanding of cybercrime incidents. The data collected through surveys and interviews, from IT professionals, and security experts who are directly engaged in the Pakistani banking sector and these existing datasets provided valuable context and background information. Collected data was unprocessed and contain some missing values in order to find out its results Data preprocessing method was used for cleaning, transforming, preparing raw data for analysis to find out accuracy and suitability for research objectives. We use ML techniques for result evaluation we use Confusion matrix. The methodology of our work is represented in mentioned below diagram.

3.1. Pre-processing Data

In data analysis, pre-processing is one of the key steps, which involves transforming and preparing data for analysis. The Data preprocessing consist of data cleaning step. In data cleaning we were remove missing values. The following mentioned below diagram represent our dataset contain zero missing value.

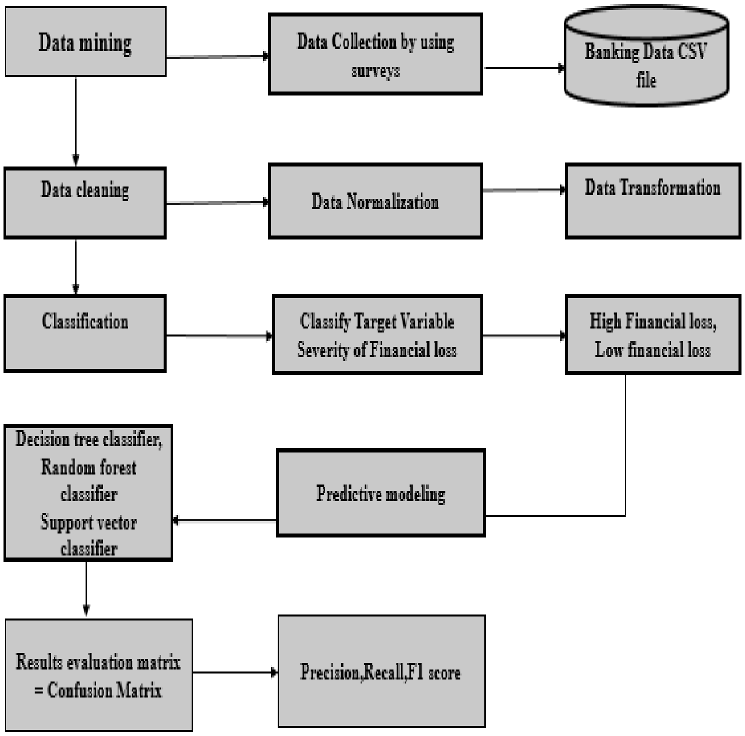
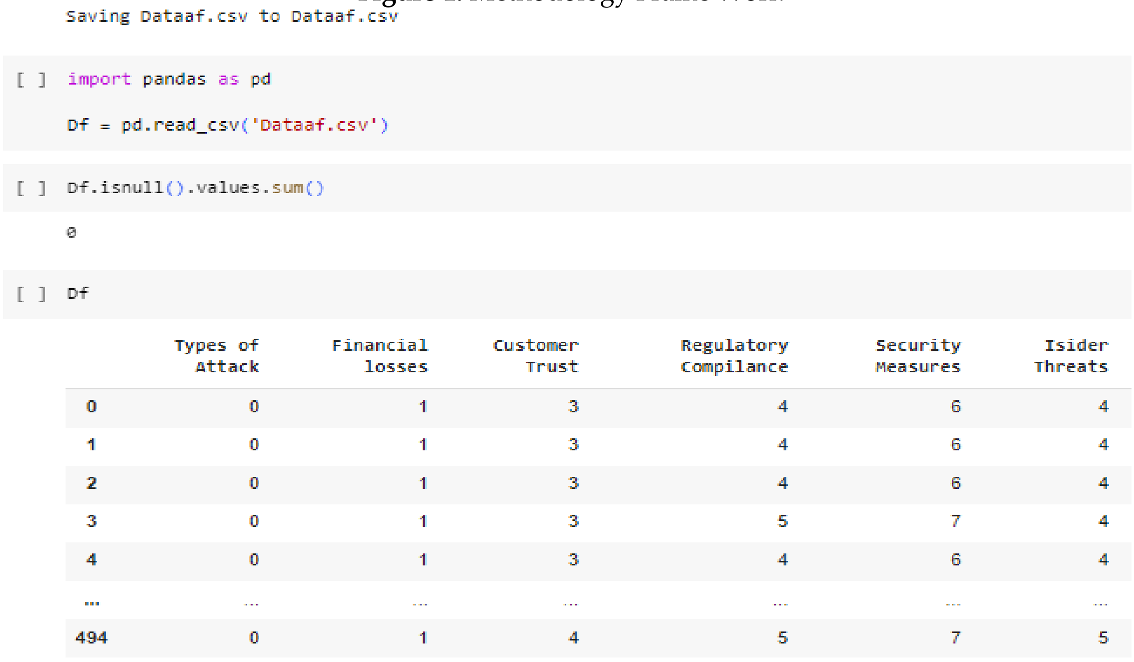

Data mining
Data Collection by using surveys
Banking Data CSV file
Data cleaning
Data Normalization
Data Transformation
Classification
Classify Target Variable Severity of Financial loss
High Financial loss, Low financial loss
Decision tree classifier, Random forest classifier Support vector classifier
Predictive modeling
Results evaluation matrix = Confusion Matrix
Precision,Recall,F1 score

Figure 1. Methodology Frame Work



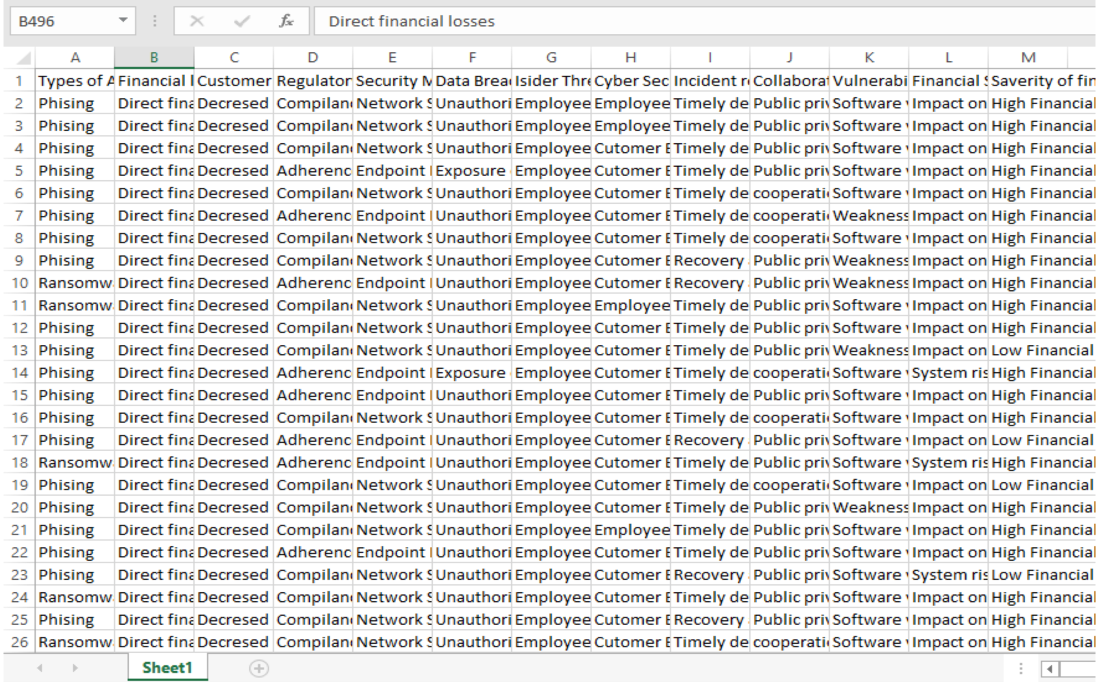
```
Saving Dataaf.csv to Dataaf.csv

[ ]  import pandas as pd

     Df = pd.read_csv('Dataaf.csv')

[ ]  Df.isnull().values.sum()

     0

[ ]  Df
```

	Types of Attack	Financial losses	Customer Trust	Regulatory Compilance	Security Measures	Isider Threats
0	0	1	3	4	6	4
1	0	1	3	4	6	4
2	0	1	3	4	6	4
3	0	1	3	5	7	4
4	0	1	3	4	6	4
...	...	...	...	...	...	...
494	0	1	4	5	7	5

Figure 2. Data Cleaning

3.2. Data without Preprocessing

Data without preprocessing are represented in mentioned below diagram.



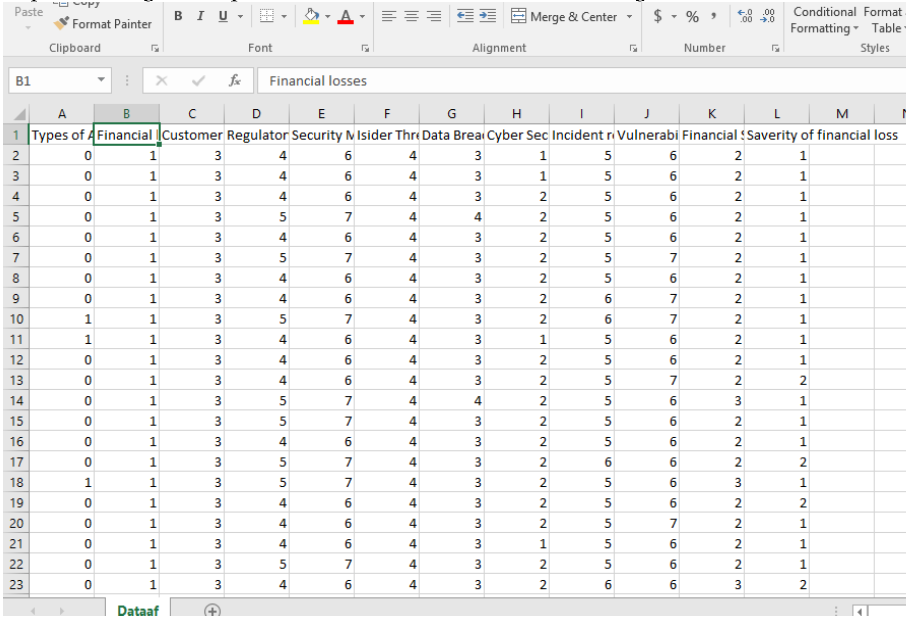
B496 | *fx* Direct financial losses

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Types of A	Financial l	Customer	Regulator	Security M	Data Brea	Isider Thre	Cyber Sec	Incident r	Collaborat	Vulnerabi	Financial S	Saverity of fin
2	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Employee	Timely de	Public pri	Software	Impact on	High Financial
3	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Employee	Timely de	Public pri	Software	Impact on	High Financial
4	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Timely de	Public pri	Software	Impact on	High Financial
5	Phising	Direct fina	Decresed	Adherenc	Endpoint I	Exposure	Employee	Cutomer E	Timely de	Public pri	Software	Impact on	High Financial
6	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Timely de	cooperati	Software	Impact on	High Financial
7	Phising	Direct fina	Decresed	Adherenc	Endpoint I	Unauthori	Employee	Cutomer E	Timely de	cooperati	Weakness	Impact on	High Financial
8	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Timely de	cooperati	Software	Impact on	High Financial
9	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Recovery	Public pri	Weakness	Impact on	High Financial
10	Ransomw	Direct fina	Decresed	Adherenc	Endpoint I	Unauthori	Employee	Cutomer E	Recovery	Public pri	Weakness	Impact on	High Financial
11	Ransomw	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Employee	Timely de	Public pri	Software	Impact on	High Financial
12	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Timely de	Public pri	Software	Impact on	High Financial
13	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Timely de	Public pri	Weakness	Impact on	Low Financial
14	Phising	Direct fina	Decresed	Adherenc	Endpoint I	Exposure	Employee	Cutomer E	Timely de	cooperati	Software	System ris	High Financial
15	Phising	Direct fina	Decresed	Adherenc	Endpoint I	Unauthori	Employee	Cutomer E	Timely de	Public pri	Software	Impact on	High Financial
16	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Timely de	cooperati	Software	Impact on	High Financial
17	Phising	Direct fina	Decresed	Adherenc	Endpoint I	Unauthori	Employee	Cutomer E	Recovery	Public pri	Software	Impact on	Low Financial
18	Ransomw	Direct fina	Decresed	Adherenc	Endpoint I	Unauthori	Employee	Cutomer E	Timely de	Public pri	Software	System ris	High Financial
19	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Timely de	cooperati	Software	Impact on	Low Financial
20	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Timely de	Public pri	Weakness	Impact on	High Financial
21	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Employee	Timely de	Public pri	Software	Impact on	High Financial
22	Phising	Direct fina	Decresed	Adherenc	Endpoint I	Unauthori	Employee	Cutomer E	Timely de	Public pri	Software	Impact on	High Financial
23	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Recovery	Public pri	Software	System ris	Low Financial
24	Ransomw	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Timely de	Public pri	Software	Impact on	High Financial
25	Phising	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Recovery	Public pri	Software	Impact on	High Financial
26	Ransomw	Direct fina	Decresed	Compilan	Network S	Unauthori	Employee	Cutomer E	Timely de	cooperati	Software	Impact on	High Financial

Figure 3. Data without Pre processing

3.3. Data with Preprocessing

Data with preprocessing are represented in mentioned below diagram



B1 | *fx* Financial losses

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Types of A	Financial l	Customer	Regulator	Security M	Isider Thre	Data Brea	Cyber Sec	Incident r	Vulnerabi	Financial S	Saverity of financial loss	
2	0	1	3	4	6	4	3	1	5	6	2	1	
3	0	1	3	4	6	4	3	1	5	6	2	1	
4	0	1	3	4	6	4	3	2	5	6	2	1	
5	0	1	3	5	7	4	4	2	5	6	2	1	
6	0	1	3	4	6	4	3	2	5	6	2	1	
7	0	1	3	5	7	4	3	2	5	7	2	1	
8	0	1	3	4	6	4	3	2	5	6	2	1	
9	0	1	3	4	6	4	3	2	6	7	2	1	
10	1	1	3	5	7	4	3	2	6	7	2	1	
11	1	1	3	4	6	4	3	1	5	6	2	1	
12	0	1	3	4	6	4	3	2	5	6	2	1	
13	0	1	3	4	6	4	3	2	5	7	2	2	
14	0	1	3	5	7	4	4	2	5	6	3	1	
15	0	1	3	5	7	4	3	2	5	6	2	1	
16	0	1	3	4	6	4	3	2	5	6	2	1	
17	0	1	3	5	7	4	3	2	6	6	2	2	
18	1	1	3	5	7	4	3	2	5	6	3	1	
19	0	1	3	4	6	4	3	2	5	6	2	2	
20	0	1	3	4	6	4	3	2	5	7	2	1	
21	0	1	3	4	6	4	3	1	5	6	2	1	
22	0	1	3	5	7	4	3	2	5	6	2	1	
23	0	1	3	4	6	4	3	2	6	6	3	2	

Figure 4. Data with Preprocessing

3.4. Data set Features

Data set Features with categories are shown in below table.

Table 2. Dataset Features

Feature	Category 1	Category 2
Type of Cybercrime	Phishing	Ransomware
Financial Losses	Direct financial losses	Indirect financial losses

Customer Trust	Decreased customer confidence	Loss of trust in security measures
Regulatory Compliance	Compliance with PCI DSS	Adherence to cybersecurity regulations
Security Measures	Network security	Endpoint protection
Data Breaches	Unauthorized data access	Exposure of sensitive financial info
Insider Threats	Employee data leaks	Insider fraud or theft by bank employees
Cybersecurity Awareness	Employee training on best practices	Customer education on cyber threats
Incident Response	Timely detection and containment	Recovery and system restoration
Collaboration	Public-private information sharing	Cooperation with law enforcement
Vulnerabilities	Software vulnerabilities	Weaknesses in authentication
Financial Stability	Impact on banking sector stability	Systemic risks from cyber threats
Severity of Financial Losses	Low Financial Losses	High Financial loss

3.5. Machine learning Methods

We use ML techniques SVC, Random Forest and Decision Tree for prediction Analysis.

3.5.1. SVC (Support vector classifier)

This popular classification algorithm seeks to find an optimal hyperplane or a set of hyperplanes that can separate instances from different classes using the Support Vector classifier (SVM). By maximizing the margin between the classes, SVMs find the hyperplane(s), which allows them to generalize to unseen data more easily. By mapping the data into higher dimensional feature spaces using kernel functions, SVM can handle linearly separable and non-linearly separable data. The method works well for binary as well as multi-class classification tasks.

3.5.2. Random Forest

With the Random Forest Classifier, multiple decision trees are combined to improve classification accuracy and robustness. During training each tree on a random subset of data and a random subset of features, it constructs an ensemble of decision trees. Based on the votes or averages of individual trees, the final prediction is made. With Random Forest, overfitting is reduced and generalization is enhanced as randomness is introduced into the tree-building process. It can handle high-dimensional datasets well as both binary and multiclass classification tasks.

3.5.3. Decision Tree

Decision Trees represent hierarchical structures of decisions and rules. They are divided into internal nodes representing features and attributes, and leaves represent class labels. Various criteria, such as information gain and Gini purity, are used to select the best splits at each node of a Decision Tree recursively. Based on the value of the features of instances, the decision tree provides a clear and interpretable set of rules for classification. Decision trees are prone to overfitting, however, so techniques like pruning and ensemble methods are often used to avoid this problem.

3.5.4. Confusion Matrix

The performance of machine learning models is usually evaluated using the Confusion Matrix, Precision, Recall, and F1 Score. Using a confusion matrix, we can summarize the performance of a classification model by identifying how many true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) were predicted. By analyzing the matrix, we can understand the model's accuracy and misclassifications. We use this matrix to evaluate the performance of the model on various categories and calculate various metrics. A confusion matrix is a table often used to describe the performance of a classification model on test data with known true values**.**

True Positive (TP): The number of positive examples that a model predicted correctly.
False Positive (FP): The number of negative examples that the model incorrectly predicted as positive.
True Negative (TN): The number of negative examples correctly predicted by the model.
False Negative (FN): The number of positive examples incorrectly predicted as negative by the model.

4. Results

4.1. Classifier Accuracy

Classifier Accuracy is given below in table Random Forest Classifier achieve highest accuracy 94%

Table 3. Result

Classifier	Accuracy %
Decision tree classifier	92%
Random forest classifier	94%
SVC	93%

4.2. Precision Recall F1 Score of Random Forest Classifier

Precision Recall F1 Score of Random Forest Classifier are shown in graph below

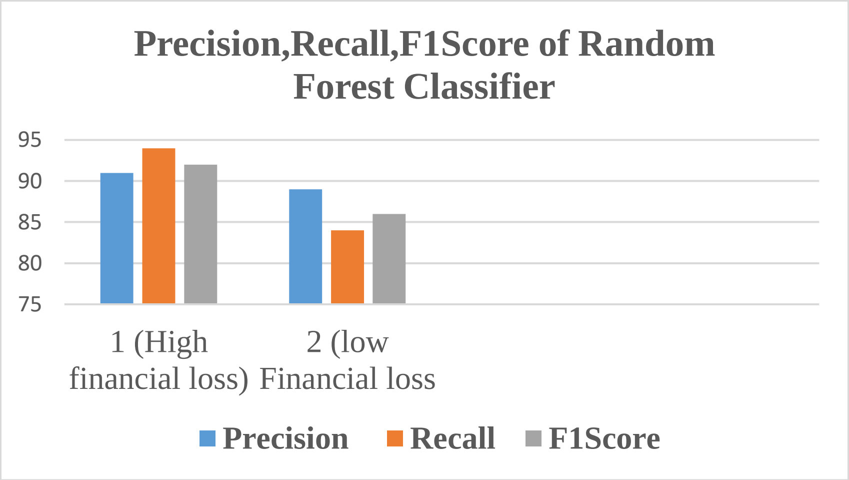


Figure 5. Random Forest Score

4.3. Precision, Recall,F1 score of Decision Tree Classifier

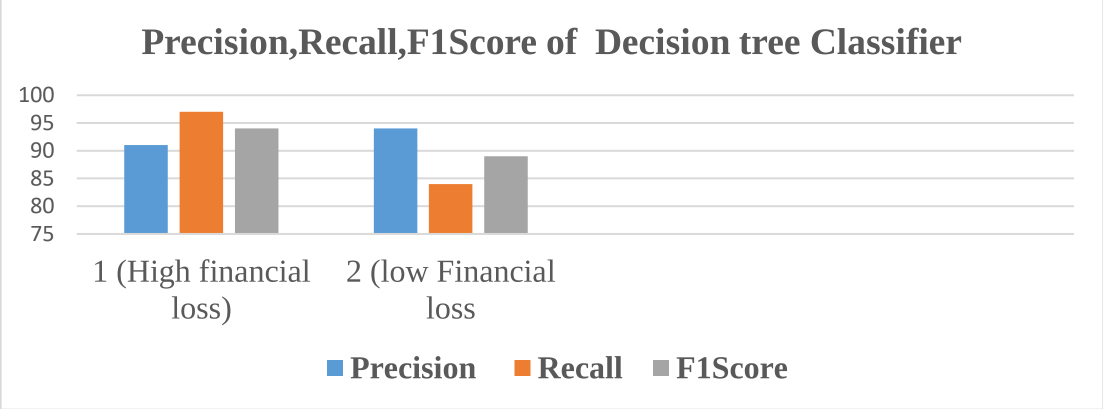


Figure 6. Decision Tree Score

4.4. Precision Recall F1score of SVC Classifier

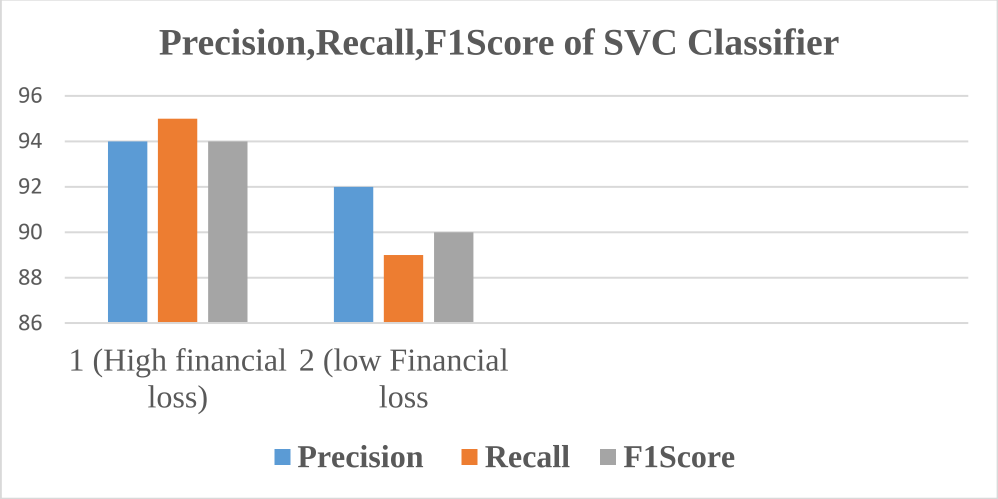


Figure 7. SVC Score

Table 4. Comparatively Analysis

Research Focus	Machine Learning	Data Analysis	Comparative Analysis	Frame work Enhancement
Cybercrime detection using ML in banking sector	Used ML techniques for the analysis of banking data, extensive analysis of cyber threats	Used ML techniques for predictive analysis	Conducted comparative analysis of different ML models and their effectiveness	Enhance existing framework by using advance Machine learning Algorithms

5. Conclusion

Pakistani banks are seriously threatened by cybercrime because of its prevalence and severity. Getting rid of cybercrime is possible if the public and private sectors collaborate and share information and work with law enforcement. It's important for financial institutions to follow cybersecurity regulations and address authentication issues. It's also important to make sure your network, endpoint, and employee security are secure. In addition, this study emphasizes the importance of comprehensive security measures to deal with cybercrime in banks. it's important to deal with cybercrime. In feature researchers can expand data sources globally to include more diverse scenarios and insights by using large data set and different ML algorithms.

References

1. Ahmad, D. A. (2011). E-banking Functionality and Outcomes of Customer Satisfaction:An Empirical Investigation.
2. Ahmed, Q. M. M. (2018). Analysis of the recent attacks on Pakistani Banks. PakCERT Threat Intelligence Report. 1(3), 20-34.
3. Ankit, S. (2011). Factors Influencing Online Banking Customer Satisfaction andTheir Importance in Improving Overall Retention Levels: An Indian Banking Perspective. Information and Knowledge Management
4. Aral, S., & Weill, P. (2007). IT assets, organizational capabilities, and firm performance: How resource allocations and organizational Effect of Cyber Security Costs on Performance of E-banking Khalid, Abid, Raheel Journal of Managerial Sciences 97 Volume 14 Issue 4 Oct-Dec 2020 differences explain performance variation. Organization science, 18(5), 763-780.
5. Arcuri, M. C., Brogi, M., & Gandolfi, G. (2014). The effect of information security breaches on stock returns: Is the cyber-crime a threat to firms? In European Financial Management Meeting. The National Academics Press, US, pp. 1–170.
6. Ayo, C. K., & Ukpere, W. I. (2010). Design of a secure unified e-payment system in Nigeria: A case study. African Journal of Business Management. Desta, Y. (2018). Customers' e-banking adoption in Ethiopia, PhD Dissertation, Addis Ababa University, Ethiopia. Fonchamnyo,
7. Bukht, T. F. N., Raza, M. A., Awan, J. H., & Ahmad, R. (2020). Analyzing cyber-attacks targeted on the Banks of Pakistan and their Solutions. IJCSNS International Journal of Computer Science and Network Security, 20(2).
8. Castelli, M., Manzoni, L. and Popovič, A., 2016. An artificial intelligence system to predict quality of service in banking organizations. Computational intelligence and neuroscience, 2016.
9. Chen, X., Chen, J., & Liu, Y. (2018). Understanding the Impact of Cybercrimes on Consumer Attitudes Toward E-Banking in China. In Proceedings of the 10th International Conference on Management of Digital EcoSystems (pp. 190-196). ACM.
10. Cidon, A., Gavish, L. and Perone, M., Barracuda Networks Inc, 2019. System and method for ai-based anti-fraud user training and protection. U.S. Patent Application 15/693,353.
11. classification. Int. J. Netw. Secur. 15 (1), 390–396. Crisanto, J.C. and Prenio, J., 2017. Regulatory approaches to enhance banks' cybersecurity frameworks. Financial Stability Institutions (FSI) Insights on policy implementation, (2). D. C. (2013). Customers' perception of E-banking adoption in Cameroon: An empirical assessment of an extended TAM. International journal of economics and finance, 5(1), 166- 176.
12. Effect of Cyber Security Costs on Performance of E-banking Khalid, Abid, Raheel Journal of Managerial Sciences 98 Volume 14 Issue 4 Oct-Dec 2020
13. Effect of cyber security related costs on development of product innovation performances and services: A case study of NIC bank of Kenya. PhD Dissertation. Kenyatta University of Agriculture and Technology.
14. Electronic Banking Adoption and Financial Performance of Commercial Banks in Kenya, Nairobi City County. International Journal of Finance and Accounting, 4(2), 19-38.
15. Gaskin, J., & Lim, J. (2016). Model fit measures. Gaskination's StatWiki, 1-55. Governance, C. (2019). Corporate Governance and Financial Performance of Nigerian Banks–PDF–Complete Project Material. Accounting & Finance. Gupta, M. (2019). A Study of Customer Awareness Towards Internet Banking. Advance and Innovative Research, 86.
16. Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. Authorea Preprints.
17. Hair, J. F., Ringle, C. M., & Sarstedt, M. (2013). Partial least squares structural equation modeling: Rigorous applications, better results & higher acceptance. Henri, J. F., & Wouters, M. (2019). Interdependence of management control practices for product innovation: The influence of environmental unpredictability. Accounting, Organizations and Society, 101073.
18. Hasham, S., Joshi, S. and Mikkelsen, D., 2019. Financial Crime And Fraud In The Age of Cyber Security. McKinsey & Company.
19. Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed big data. Journal of Management Analytics, 5(4), 256-275.
20. Hu, L. T., Bentler, P. M., & Hoyle, R. H. (1995). Structural equation modeling: Concepts, issues, and applications. Evaluating model fit, 54, 76-99.
21. Hussain, A., Qureshi, M. A., Arshad, N., & Rizwan, M. (2020). Factors Affecting E-Banking Adoption: Evidence from Pakistan. Academy of Strategic Management Journal, 19(6), 1-11.

22. Islam, S., Kabir, M. R., Dovash, R. H., Nafee, S. E., & Saha, S. (2019). Impact of Online Banking Adoption on Bank's Profitability: Evidence from Bangladesh. European Journal of Business and Management Research, 4(3). Jepchumba, P., & Simiyu, E. (2019).
23. Jakšič, M. and Marinč, M., 2019. Relationship banking and information technology: The role of artificial intelligence and FinTech. Risk Management, 21(1), pp.1-18.
24. Jamshed, J., Rafique, W., Baig, K., & Ahmad, W. (2022). Critical Analysis of Cybercrimes in Pakistan: Legislative Measures and Reforms. International Journal of Business and Economic Affairs, 7(1), 10-22.
25. Kanabolo, D. and Gundeti, M.S., 2019. The Role of Artificial Intelligence (AI) in Medical Imaging: General Radiologic and Urologic Applications. Medical Imaging: Artificial Intelligence, ImageRecognition, and Machine Learning Techniques, p.27.
26. Kurode, T., 2018. Review of Applicability of Artificial Intelligence in Various Financial Services in India. Journal of Advance Management Research, 6.
27. Lekha, K. C., & Prakasam, S. (2017, August). Data mining techniques in detecting and predicting cybercrimes in banking sector. In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) (pp. 1639-1643).
28. Mehmood, N., Shah, F., Azhar, M., & Rasheed, A. (2014). The factors effecting e-banking usage in Pakistan. Journal of Management Information System and E-commerce, 1(1), 57-94.
29. Menon, N. M., & Lee, B. (2000). Cost control and production performance enhancement by IT investment and regulation changes: evidence from the healthcare industry. Decision Support Systems, 30(2), 153-169.
30. Mohamud, A. A., & Mungai, J. (2019). Financial innovation on performance of commercial banks in Garissa County, Kenya. Strategic Journal of Business & Change Management, 6(1), 491-504.
31. Nazaritehrani, A., & Mashali, B. (2020). Development of E-banking channels and market share in developing countries. Financial Innovation, 6(1), 12. Njoroge, E. W. (2017).
32. Nobanee, H., Dilshad, M. N., Al Dhanhani, M., Al Neyadi, M., Al Qubaisi, S., & Al Shamsi, S. (2021). Big data applications the banking sector: A bibliometric analysis approach. Sage Open, 11(4), 21582440211067234.
33. Padmaavathy, P. A. (2019). Cyber Crimes: A Threat To The Banking Industry. International Journal of Management Research and Reviews, 9(4), 1-9.
34. Prabowo, H.Y., 2011. Building our defence against credit card fraud: a strategic view.
35. Primer, A., 2016. Cybersecurity plans and strategies, establishing priorities, organizing
36. PwC Report, 2016. Banking in Africa Matters – African Banking Survey. Global
37. PwC Report, 2018. Global Economic Crime Survey: Pulling Fraud Out of the Shadows,
38. PwC Report, 2019. The Future of Banking: A South African Perspective [Online] Available at. www.pwc.ac.za. (Accessed 31 July 2021). Accessed.
39. PwC's Global Economic Crime Survey, 2020. Global Economic Crime and Fraud Survey, seventh ed., pp. 1–32 [Online] Available at. https://www.corruptionwatch.org.za
40. Rafiq, M., Zhang, X.-P., Yuan, J., Naz, S., Maqbool, S., 2020. Impact of a balanced
41. Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. International Journal of Current Research & Academic Review, 2(2), 173-178.
42. Rahman, M. M., & Ahad, M. A. (2019). Factors Influencing the Adoption of E-Banking in Bangladesh: An Empirical Analysis. International Journal of Scientific and Research Publications, 9(6), 515-522.
43. Rajapathirana, R. J., & Hui, Y. (2018). Relationship between innovation capability, innovation type, and firm performance. Journal of Innovation & Knowledge, 3(1), 44-55
44. Ramamoorti, S., Morrison, D., Koletar, J.W., 2014. Bringing freud to fraud. J. Foren.Rezaee, Z., 2005. Causes, consequences, and deterrence of financial statement fraud. Crit.Perspect. Account. 16 (3), 277–298.
45. Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trend. World Journal of Advanced Research and Reviews, 15(1), 138-156.