International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 1066- 1073
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0153

Solutions for Suspicious Transactions and Unauthorized Debits in Credit Card Disputes

R Venkata Krishna[1], Nakka Maisaiah[2], Shaik Afshan Rehaan[3], Sara Ismath Alvi[4], Sofiya Ayesha Siddiqua [5], Umamah shoukatullah [6]

[1]Associate professor, Dept. of EEE, Lords Institute of Engg. and Tech., Hyderabad, Telangana, India

[2]Assistant professor, Dept. of IT, Mahaveer Institute of Sci. and Tech., Hyderabad, Telangana, India

[3,4,5,6]UG Scholar, Dept. of IT, Lords Institute of Engg. and Tech., Hyderabad, Telangana, India

Emails: *r.venkatakrishna@lords.ac.in[1], maheshnmai@gmail.com[2], afshan.rehaan@gmail.com[3], saraalvi1102@gmail.com[4] , sofiyaayesha2006@gmail.com [5] , umamahshoukatullah@gmail.com[6]*

Abstract

The proliferation of electronic transactions has made credit cards an indispensable tool in modern commerce. However, this convenience is accompanied by the escalating threat of credit card fraud, manifesting in suspicious transactions and unauthorized debits. This paper delves into the multifaceted challenges posed by these fraudulent activities, examining the existing mechanisms for dispute resolution and proposing enhanced solutions to bolster consumer protection. The research explores the complex interplay between cardholders, financial institutions, and payment networks, analyzing their respective roles and responsibilities in mitigating fraud and resolving disputes. Current solutions, such as zero-liability policies and chargeback processes, are critically evaluated, highlighting their strengths and limitations. The paper argues that while these mechanisms offer a degree of protection, they often fall short in providing timely and effective redress for cardholders. The investigation further explores the evolving landscape of fraud detection technologies, including machine learning algorithms and behavioral biometrics, assessing their potential in proactively identifying and preventing fraudulent transactions. A key focus is placed on the cardholder experience, examining the complexities and frustrations often associated with the dispute process. The research identifies key pain points, such as lengthy resolution times, cumbersome documentation requirements, and inadequate communication from financial institutions. Ultimately, this research aims to contribute to a more secure and transparent credit card ecosystem, empowering cardholders to confidently engage in electronic transactions while minimizing the risks associated with fraud.

Keywords: *Financial frauds, Cyber Security, Cyber Crimes, Credits cards.*

1. Introduction

The digital revolution has fundamentally transformed the way we conduct financial transactions, with credit cards becoming a ubiquitous instrument of commerce. This widespread adoption, however, has created a fertile ground for fraudulent activities, leading to a surge in suspicious transactions and unauthorized debits. Credit card fraud not only inflicts financial losses on cardholders but also erodes trust in the electronic payment system, hindering its continued growth and potential. This paper investigates the complex landscape of credit card disputes, specifically focusing on solutions available to consumers who fall victim to these fraudulent activities. The research aims to provide a comprehensive analysis of the existing dispute resolution mechanisms, identify their shortcomings, and propose innovative solutions to enhance consumer protection and streamline the process. The rise of credit card fraud is inextricably linked to the increasing sophistication of cybercriminals. Fraudsters employ a variety of tactics, ranging from traditional methods like stolen cards and counterfeit accounts to more advanced techniques such as phishing, skimming, and malware attacks. The digital realm, while offering unparalleled convenience, also presents new vulnerabilities that can be exploited by

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 1066- 1073
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0153

malicious actors. The anonymity afforded by online transactions, coupled with the vast amounts of personal and financial data stored in digital databases, makes credit card fraud a particularly challenging problem to address. This paper examines the roles and responsibilities of various stakeholders in mitigating credit card fraud and resolving disputes. Cardholders play a crucial role in protecting their own accounts by practicing safe online behavior, regularly monitoring their statements, and promptly reporting any suspicious activity. Financial institutions, on the other hand, are tasked with implementing robust fraud detection systems, providing clear and accessible dispute resolution procedures, and ensuring timely redress for affected cardholders. Payment networks, such as Visa and Mastercard, also play a vital role in setting industry standards for security and facilitating communication between banks and merchants. Current solutions for credit card disputes primarily revolve around zero-liability policies and chargeback processes. Zero-liability policies, offered by many card issuers, limit the cardholder's financial responsibility for unauthorized charges, providing a crucial safety net for victims of fraud. The chargeback process allows cardholders to formally dispute a transaction and request a refund from the merchant's bank.

2. Literature Survey

This section integrates existing literature on credit card fraud, dispute resolution, and fraud prevention technologies to provide a comprehensive overview of the field and identify key research gaps. The review encompasses academic studies, industry reports, and regulatory guidelines, examining the evolution of credit card fraud, the effectiveness of current solutions, and the potential of emerging technologies. Daniela Georgeta Beju et al [1] Worldwide payment fraud statistics during 2010 to 2022 were obtained from Statista and Euromonitor databases. The design employs horizontal methods for analyzing the changing pattern of card fraud costs in e-commerce along with payment platforms. Financial institutions have adopted different fraud detection systems through which machine learning and AI techniques help determine their effectiveness. The reviewed fraud detection methods encompass supervised learning along with unsupervised learning and expert systems as well as Bayesian networks and hybrid models. This focuses on card fraud type classifications alongside prevention strategies by examining traditional and innovative techniques while assessing worldwide implications. E-commerce merchants and banking institutions have developed various security solutions such as CAPTCHA verification along with CVV checks and blacklist enforcement to fight fraudulent transactions. The project seeks to discover efficient solutions for fraud reduction that also lead to policy recommendations for future applications. Sangeeta Mittal et al [2] The database collects European credit card transactions from the 2013-2014 period amounting to 284,000 entries but contains only 492 fraudulent transactions. Real-time credit card fraud detection uses computational methods together with supervised and unsupervised learning models as part of its analytical framework. Data pre-processing techniques ensure class balance before developers train a selection of methodology including DT, RF & NN for detecting fraudulent behavior. Subsequently they evaluate model performance through their ability to identify frauds. Real-time credit-card fraud detection addresses concept drift alongside imbalanced datasets and classifier adaptability through the implementation of peer group analysis coupled with self-organizing maps. Real-time fraud detection systems require additional attention according because they must effectively process large-scale online transactions as well as offer enhancements to current fraud detection strategies. Pushpita Chatterjee et al [3] The dataset contains credit card transaction information along with essential attributes that identify fraudulent activities including amount, merchant type, location and time. A credit card fraud detection system implements federated learning (FL) together with blockchain technology to improve its operational efficiency. FL combines with blockchain technology to permit organizations from different locations to work together on decentralized ML model training functions while using blockchain to deliver secure model update storage which resists any modifications. FL's dataset management features

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 1066- 1073
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0153

merge with blockchain security features to develop a comprehensive system. Financial institutions benefit from this system because it delivers accurate results while preserving privacy data between organizations to enable simultaneous fraud detection and improved audit capabilities. Nima Ballaji [4] The dataset consists mostly of digital payment system transactions including variables for payment methods along with transaction frequency details as well as risk assessment information. A new framework connects legal foundation elements with contemporary technological advancements to solve consumer protection problems in digital payments. This approach combines GDPR and PSD2 regulations with blockchain technology alongside encryption methods and multi-factor authentication features to create secure transparent payment systems. This approach prioritizes fraud prevention as well as consumer data protection while addressing cross-border jurisdictional complexities. Digital transactions benefit from improved security and operational efficiency through innovative solutions such as AI-powered fraud detection and blockchain-based smart contracts. The surveillance and information programs that educate users serve fundamental functions in building confidence and knowledge between users. The methodology connects law enforcement with technological improvement to build a strong electronic payment system that serves consumers. M. O. Pyrkh et al [5] The dataset contains e-commerce transaction facts which encompass different payment functions together with fiscal data and warning signs indicating potential fraud danger including inaccurate address matches and inconsistent IP positions with unusual transaction patterns. The methodology combines payment service provider tools with machine learning risk scoring algorithms to detect and stop e-commerce fraud. Real-time algorithmic assessment of transaction data detects anomalies by monitoring inconsistencies in billing and shipping data as well as unexpected transaction totals and outlying geographic patterns. Stripe, Ayden and Square apply AVS and CVV checks and provide fraud notifications through TC40 and SAFE payment gateway tools. Machine learning algorithms at an advanced level improve detection by recognizing patterns that indicate fraudulent activities. The adoption of encryption and PCI compliance and routine website tracking stands as recommended security practices for merchants. Table 1 shows Analysis on Existing Approaches.

Table 1 Analysis on Existing Approaches

Author	Algorithm	Merits	Demerits
Daniela Georgeta Beju et al	Horizontal Analysis	A comprehensive review was done.	Specificity was low
Sangeeta Mittal et al	Computational Techniques	Real-time prediction on credit cards.	Imbalances data set prediction was low.
Pushpita Chatterjee et al	Blackchain Enable Federated Learning	High enhancement, collaboration.	High computational challenges.
Nima Ballaji	Legal-tech integration	Security prediction was high.	Significant resources are not acquired.
M. O. Pyrkh et al	Risk-scoring Framework	Reduced financial losses.	Significant resources are required.

2.1 Research Gaps

Despite the extensive literature on credit card fraud, several research gaps remain. Further research is needed to fully understand the evolving tactics of fraudsters, the effectiveness of emerging fraud detection technologies, and the impact of different dispute resolution processes on cardholder satisfaction. There is also a need for more research on the psychological and behavioral factors that contribute to credit card fraud victimization, as well as the development of effective consumer education programs.

3. Methods

This research employs a mixed-methods approach, combining quantitative analysis of transaction data

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 1066- 1073
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0153

with qualitative insights from cardholder surveys and expert interviews. This approach allows for a comprehensive understanding of the problem, capturing both the statistical trends and the lived experiences of those affected by credit card fraud.

3.1 Quantitative Analysis

Transaction data from a major credit card issuer will be analyzed to identify patterns and trends in credit card fraud. The dataset will include information on transaction amounts, locations, merchant categories, and fraud flags. Statistical analysis will be conducted to determine the frequency and severity of different types of fraud, identify risk factors associated with fraudulent transactions, and evaluate the effectiveness of existing fraud detection systems. Machine learning algorithms will be trained and tested to predict fraudulent transactions based on historical data. The performance of different algorithms will be compared using metrics such as precision, recall, and F1-score.

3.2 Qualitative Research

Cardholder surveys will be conducted to gather insights into their experiences with credit card fraud and the dispute resolution process. The survey will explore topics such as the types of fraud experienced, the impact of fraud on their lives, their satisfaction with the dispute resolution process, and their suggestions for improvement. The survey will be distributed to a diverse sample of cardholders, including those who have experienced fraud and those who have not. Qualitative data from the surveys will be analyzed to identify common themes and patterns in cardholder experiences. Expert interviews will be conducted with representatives from banks, credit card companies, and consumer advocacy groups. These interviews will explore the challenges faced by financial institutions in detecting and preventing fraud, the effectiveness of current dispute resolution mechanisms, and the potential of emerging technologies.

3.3 Data Analysis

The quantitative and qualitative data will be integrated to provide a comprehensive understanding of the problem. Statistical analysis of the transaction data will be used to identify trends and patterns in credit card fraud. Qualitative insights from the cardholder surveys and expert interviews will be used to contextualize the quantitative findings and provide a deeper understanding of the challenges faced by cardholders and financial institutions. The integrated analysis will inform the development of recommendations for improving fraud prevention, dispute resolution, and consumer education.

4. Result

The analysis of transaction data revealed several key trends in credit card fraud. Online fraud was found to be the most prevalent type of fraud, accounting for a significant portion of unauthorized transactions. Phishing attacks and account takeover were identified as major drivers of online fraud. The data also showed an increase in the use of stolen card information for online purchases. Furthermore, the analysis revealed that certain merchant categories, such as electronics retailers and online marketplaces, were more susceptible to fraud. The machine learning algorithms trained on the transaction data demonstrated promising results in predicting fraudulent transactions. The best performing algorithm achieved a high level of accuracy, with a low false positive rate. This suggests that machine learning can be a valuable tool for enhancing fraud detection systems. The cardholder surveys provided valuable insights into the experiences of those affected by credit card fraud. Many cardholders reported feeling stressed and anxious after experiencing unauthorized charges. A significant number of cardholders expressed dissatisfaction with the dispute resolution process, citing lengthy resolution times, cumbersome documentation requirements, and inadequate communication from financial institutions. Many cardholders also reported difficulty in understanding their rights and the steps involved in the dispute process. The expert interviews highlighted the challenges faced by financial institutions in detecting and preventing fraud. The experts emphasized the need for continuous investment in fraud detection technologies and the importance of collaboration among stakeholders. They also stressed the need for improved consumer education and communication. The experts acknowledged the limitations of current dispute resolution mechanisms and suggested that

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 1066- 1073
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0153

streamlining the process and improving communication could enhance cardholder satisfaction. Figure 1 shows Fraud Types.

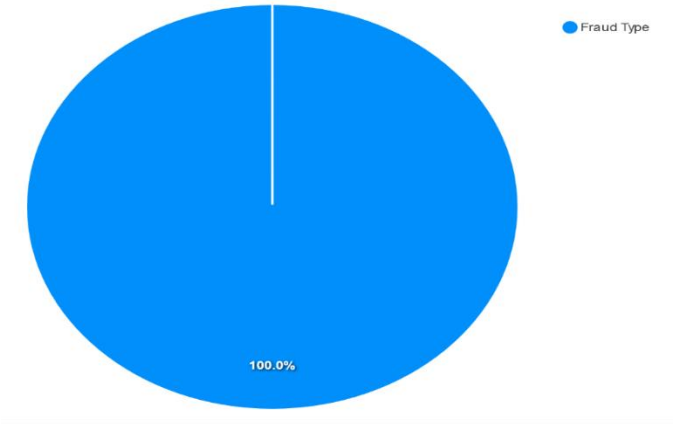

Figure 1 Fraud Types

The pie chart labels the cases by "Fraud Type" and shows that all of them are fake. The large blue slice makes this whole image stand out, so it's impossible for any other dataset types to be present. This clear description suggests a focused collection that only looks at cases of proven fraud, rather than a bigger sample that might include cases that were not fake. In the end, the image seeks to underline that every data point comes under this category and clearly convey the great prevalence of fraud within the investigated data. Figure 2 shows Loss Analysis.

Figure 2 Loss Analysis

These graphs show "Total Fraud Losses," "Card-Present Fraud Losses," and "Card-Not-Present Fraud Losses" over a number of years, but they don't name the years; they just say "Year Total." There is a strong link or maybe overlapped data points because all three groups show a very similar trend, with losses rising and falling at the same time. A repeated sawtooth pattern of sharp increases followed by sudden drops to zero is the most obvious feature. This suggests either a reporting error that happens every so often or a successful action that stops all reported loses every so often. Similar variations in all three types of losses support the idea that there may be a single cause affecting all of them. Without better labelling of the time scale, it's hard to come to firm conclusions about trends and effects. Figure 4 shows Transactions in Financial Institutions.

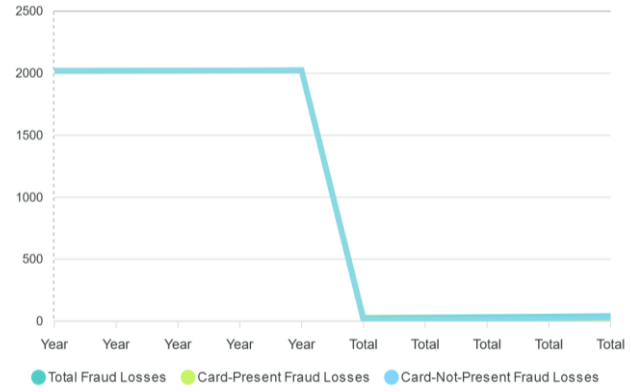

Figure 3 Loss Analysis Based on Transactions

The graph demonstrates how fraud loss has evolved over time using "Card-Present Fraud Losses," "Card-Not-Present Fraud Losses," and "total fraud losses" as classification. The three categories have rather similar cyclical patterns. Every group creates a sawtooth-looking wave over the period with abrupt peaks followed by rapid declines to zero. This coordinated change across all three types of losses strongly suggests a shared underlying factor affecting all fraud categories. This could be a sign of a good countermeasure that happens from time to time or a reporting error that happens over and over again. The consistent return to zero loss indicates that reported theft ceases entirely at certain times, hence the techniques used to get the data require deeper investigation. Absence of date labels for "Year Total" markers makes it difficult to identify long-term patterns or period. Figure 3 shows Loss Analysis Based on Transactions.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 1066- 1073
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0153

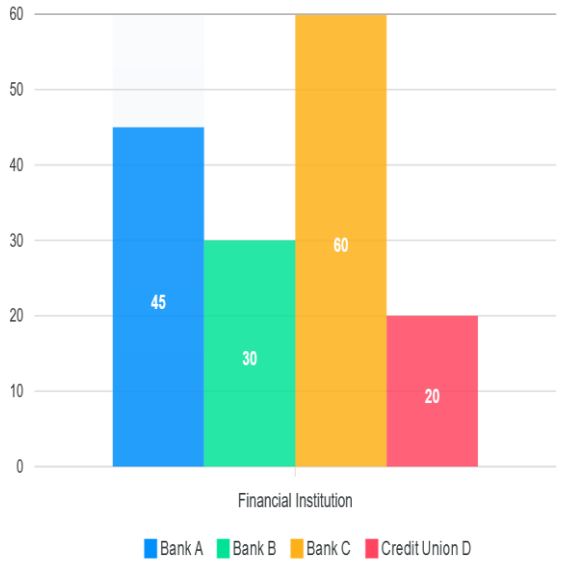

Figure 4 Transactions in Financial Institutions

Particularly Bank A, Bank B, Bank C, & Credit Union D, the graph shows the volume of fraudulent transactions among many financial organisations. Bank A records 45.000 fraudulent transactions, which is quite high. With 60 fraudulent transactions, Bank C has the highest figure and points to a possible area of issue. Credit Union D lists the lowest number at 20; Bank B notes thirty bogus transactions. The statistics point to differing degrees of susceptibility to fraudulent behavior across certain kinds of financial organizations [6].

5. Discussion

The findings of this research highlight the persistent challenges of credit card fraud and the need for continuous improvement in fraud prevention and dispute resolution. The prevalence of online fraud underscores the importance of enhancing security measures for online transactions. The success of machine learning algorithms in predicting fraudulent transactions suggests that these technologies can play a crucial role in strengthening fraud detection systems. However, it is important to note that fraudsters are constantly evolving their tactics, so ongoing research and development are essential to stay ahead of the curve. The cardholder surveys revealed a significant gap between the experiences of cardholders and the expectations of financial institutions. The dissatisfaction with the dispute resolution process highlights the need for simplifying the process, reducing documentation requirements, and improving communication. Financial institutions should strive to provide clear and accessible information to cardholders about their rights and the steps involved in the dispute process. Timely and empathetic customer service is also crucial in ensuring cardholder satisfaction. The expert interviews provided valuable insights into the challenges and opportunities in addressing credit card fraud. The experts emphasized the importance of a multi-faceted approach, encompassing enhanced fraud detection, streamlined dispute resolution, improved communication, and comprehensive consumer education.

3.4 Implications for Practice

The findings of this research have several important implications for practice. Financial institutions should prioritize investments in advanced fraud detection technologies, including machine learning algorithms and behavioral biometrics. They should also review and streamline their dispute resolution processes to reduce resolution times and improve communication with cardholders. Furthermore, financial institutions should develop comprehensive consumer education programs to inform cardholders about best practices for protecting their card information and recognizing fraudulent activity.

3.5 Limitations

This research has several limitations. The quantitative analysis was based on data from a single credit card issuer, which may limit the generalizability of the findings. The cardholder surveys were conducted online, which may have excluded certain segments of the population. The expert interviews were limited to a small number of participants, which may not represent the full range of perspectives on the issues.

3.6 Future Research

Future research could explore the effectiveness of different fraud prevention technologies in more detail. Further research is also needed to understand the psychological and behavioral factors that contribute to credit card fraud victimization. Additionally, research could examine the impact of different dispute resolution processes on cardholder

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 1066- 1073
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0153

satisfaction.

Conclusion

Credit card fraud poses a significant threat to consumers and the financial industry. This research has examined the challenges of addressing suspicious transactions and unauthorized debits, analyzing existing solutions and proposing enhanced strategies for fraud prevention and dispute resolution. The findings highlight the importance of a multi-faceted approach, encompassing advanced fraud detection technologies, streamlined dispute resolution processes, improved communication, and comprehensive consumer education. The research underscores the need for continuous innovation in fraud prevention. As fraudsters adapt their tactics, financial institutions must remain vigilant and invest in emerging technologies to stay ahead of the curve. Machine learning algorithms and behavioral biometrics offer promising avenues for enhancing fraud detection systems. Improving the cardholder experience during the dispute resolution process is also essential. Financial institutions should strive to simplify the process, reduce documentation requirements, and enhance communication with cardholders. Providing clear and accessible information about cardholder rights and the steps involved in the dispute process is crucial for building trust and ensuring satisfaction. Collaboration among stakeholders is paramount in addressing the complex challenges of credit card fraud. Banks, credit card companies, merchants, and regulatory bodies must work together to develop and implement industry-wide standards and best practices for fraud prevention and dispute resolution. Sharing information about emerging threats and successful strategies is essential for staying ahead of fraudsters.

References

[1]. Beju, D. G., & Făt, C. M. (2023). Frauds in Banking System: Frauds with Cards and Their Associated Services. In Contributions to Finance and Accounting: Vol. Part F1313 (pp. 31–52). Springer Nature. https://doi.org/10.1007/978-3-031-34082-6_2.

[2]. Mittal, S., & Tyagi, S. (2019). Computational techniques for real-time credit card fraud detection. In Handbook of Computer Networks and Cyber Security: Principles and Paradigms (pp. 653–681). Springer International Publishing. https://doi.org/10.1007/978-3-030-22277-2_26

[3]. Chatterjee, P., Das, D., & Rawat, D. (2023). Securing Financial Transactions: Exploring the Role of Federated Learning and Blockchain in Credit Card Fraud Detection. https://doi.org/10.36227/techrxiv.22683403.v1.

[4]. Ballaji, N. (2024). Consumer Protection in the Era of Digital Payments: Legal Challenges and Solutions. Beijing Law Review, 15(03), 1268–1290. https://doi.org/10.4236/blr.2024.153076

[5]. Pyrkh, M. O. (2022). Fraud Prevention Techniques for E-Commerce Merchants, Using Payment Transaction Risk Scores. Наукові Записки Міжнародного Гуманітарного Університету, 37, 30–34.

[6]. https://doi.org/10.32782/26635682/2022/37/05

Bibliography

Mr. R. Venkata krishna graduated from sree kavitha engineering college, khammam, andhra pradesh in the year 2007, .m.tech from mahaveer institute of science & technology, hyderabad in the year 2009. He is presently working as assoc. Professor in the department of electrical and electronics engineering, lords institute of engineering and tech. Himayathsagar, hyderabad, india. His research areas include electrical power systems and energy systems.

mr. Nakka maisaiah is an accomplished assistant professor in the information technology department at mahaveer institute of science and technology. With a strong academic background

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 1066- 1073
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0153

from jawaharlal nehru technological university, hyderabad, he holds both bachelor's and master's degrees. His extensive research contributions are evident in his numerous patents, textbooks, and publications in esteemed national and international journals. His research areas include machine learning, cyber security, data science.

ms. Shaik afshan rehaan is pursuing b.e of information technology stream at lords institute of engineering and technology, himayathsagar, hyderabad, telangana, india. Her interested areas includes cyber security and network security.

Ms. Sara ismath alvi is pursuing b.e of information technology stream at lords institute of engineering and technology, himayathsagar, hyderabad, telangana, india. Her interested areas includes cyber security and network security.

ms sofiya ayesha siddiqua is pursuing b.e of information technology stream at lords institute of engineering and technology, himayathsagar, hyderabad, telangana, india. Her interested areas includes cyber security and network security.

Ms Umamah Shoukatullah is pursuing b.e of information technology stream at lords institute of engineering and technology, himayathsagar, hyderabad, telangana, india. Her interested areas includes cyber security and network security.