Detection Of Identity Theft In Credit Card Application Forms Through Data Mining Techniques Utilizing Multilayer Algorithms

Mr. Amol Jagdish Shakadwipi[1]*, Dr.Dinesh Chandra Jain[2], Dr.S. Nagini[3]

Abstract:

Due to the unpredictable nature of the market, the deceleration in economic growth, and the swift surge of digital e-commerce, the issue of fraud has gained extensive prevalence. As electronic commerce technology continues to rapidly evolve, credit card usage has witnessed a surge, establishing it as the preferred payment method for both online and offline transactions. Consequently, the escalation of credit card fraud has emerged, impacting customers seeking smart cards and loans, who now have the option to apply for credit cards through online channels or traditional paper forms. Regrettably, these application processes have brought to light occurrences of fraudulent activities, notably identity theft, posing a critical concern for both credit cardholders and financial institutions. Ill-intentioned individuals are illicitly acquiring customers' identities and gaining unauthorized access to credit cards, thereby exposing substantial risks for both customers and financial entities.

Nonetheless, the current strategies reliant on business rules and scorecards for fraud detection, excluding data mining, have exhibited shortcomings. In response to these limitations, this research introduces an innovative approach for real-time fraud detection during the application phase. This approach entails the implementation of a novel multi-layer fraud tracking system

[1]*Research Scholar, Department of Computer Science and Engineering, Oriental University, Indore, Orcid Id : 0009-0009-1477-2005

[2]Professor, Department of Computer Science and Engineering, Oriental University, Indore, Email: dineshjain25210@gmail.com, Orcid Id :0000-0001-8990-8127

[3] Professor, Department of Computer Science and Engineering, VNR Vignana Jyothi Institute of Engineering & Technology, Hydrabad,
Department of Computer Science and Engineering, Oriental University, Indore, Email: nagini_s@vnrvjiet.in Orcid Id: 0000-0002-5699-3801

***Corresponding Author:** Mr. Amol Jagdish Shakadwipi
*Research Scholar, Department of Computer Science and Engineering, Oriental University, Indore,
Orcid Id : 0009-0009-1477-2005

founded on data mining algorithms. This system incorporates two distinct algorithms, namely communal tracing and spike tracing, synergizing to enhance the precision, swiftness, and efficiency of fraud detection procedures. By validating applications in real-time upon submission, this system serves as a robust deterrent against the approval of fraudulent credit card applications prior to issuance.

Keywords: *Multi-layer fraud tracking system, swift surge, Communal tracing,, Spike tracing.*

Introduction :

In an era marked by the rapid evolution of information technology and communication channels, instances of fraudulent activities have witnessed a global upsurge. As such, the imperative for organizations to engage in fraud tracing has intensified, given its pivotal role in augmenting the operational costs. Among these deceitful practices, identity theft stands out—a form of fraud wherein an individual assumes another person's identity, procuring their personal particulars to illicitly access resources or secure credit and privileges in the victim's name. The repercussions can be dire if the victim is wrongly held responsible for the malefactor's deeds, potentially leading to severe penalties. This nefarious act unfolds when an individual unlawfully deploys someone else's personally identifiable information, encompassing facets like name, social security number, or credit card details, to perpetrate fraud or other unlawful activities.

Identity fraud, which centers on credit applications, has surged due to the proliferation of personal data on the internet and the insecurity of conventional mail systems. Perpetrators can adeptly conceal their true identities, capitalizing on the dual nature of credit applications—accessible both online and in physical form—which can be exploited if not adequately safeguarded or disposed of. The consequences ripple through economies at a national scale. To curb these deceitful exploits and curtail financial losses, numerous enterprises have embraced sophisticated analytical methodologies. Within this landscape, data mining has emerged as a potent tool for uncovering fraudulent under takings. By meticulously dissecting extensive datasets, data mining excavates invaluable patterns and insights, facilitating the construction of predictive models. This intricate process entails the meticulous curation and exploration of data to unearth hitherto concealed trends and patterns. Although not novel, with established applications in credit scoring and fraud mitigation among financial institutions, data mining harbors manifold techniques for tracing, encompassing domains like counterfeit detection in online credit card applications. This study sets out to underscore the potency of data

mining techniques in the realm of credit application fraud tracing systems, synergizing the spike tracing and communal tracing methodologies to reinforce effectiveness.

Literature Survey :

In the contemporary landscape, the Internet has become an integral part of daily life, enabling a broad spectrum of activities and collaborations through network services like web-based platforms. This shift has led to the widespread deployment of web services, powering applications spanning online banking, social networks, cloud computing, and e-commerce.

Fraud, characterized by deliberate deception for personal gain or causing harm to others, has seen a global increase, necessitating effective tracing methods due to the resulting higher operational costs. Identity theft, a prevalent form of fraud, involves perpetrators illicitly using stolen personal information to impersonate innocent individuals. The stolen data may be either genuinely pilfered from the victim (identity theft) or artificially created by adversaries to deceive systems (synthetic identity fraud). This issue extends to instances where unauthorized individuals exploit victims' financial information, such as withdrawing funds or applying for loans under false pretenses. Instances of identity theft often involve stolen data or fraud committed by individuals known to the victim who have access to their financial documents.

Identity theft, a grave concern in the realm of digital transactions, has fueled the exploration of innovative techniques to counter fraudulent activities. Credit card application forms have become a prime target for identity theft, necessitating robust detection mechanisms to safeguard users and financial institutions. This literature survey delves into the research landscape surrounding the detection of identity theft in credit card applications using data mining techniques, particularly focusing on the utilization of multilayer algorithms for enhanced accuracy and effectiveness.The surge in digitalization and online transactions has brought convenience and efficiency but has also opened doors to malicious actors seeking to exploit vulnerabilities. The central objective of this survey is to comprehensively explore the various studies, methodologies, and advancements in the field of identity theft detection within the context of credit card applications.

By leveraging data mining, researchers and practitioners aim to uncover hidden patterns and anomalies in application forms, subsequently enabling timely fraud prevention.Scholars have

recognized the gravity of identity theft and its implications for both individuals and financial institutions. Conventional methods of fraud detection, such as rule-based systems, have shown limitations in their adaptability to evolving attack vectors. Consequently, a shift towards data mining techniques has gained prominence due to their capacity to process large volumes of data and extract meaningful insights.The exploration begins with a retrospective analysis of seminal works addressing fraud detection and identity theft, with a specific emphasis on credit card application processes. Early efforts aimed to lay the foundation by utilizing classification algorithms to distinguish between legitimate and fraudulent applications. As the field evolved, researchers ventured into multilayer algorithms, which exhibit superior performance by combining multiple detection methods, each focusing on distinct aspects of identity theft. This layered approach contributes to a holistic and effective detection mechanism.Moreover, studies have emphasized the significance of feature selection and data preprocessing to enhance the accuracy of detection models. Techniques such as ensemble learning and deep learning have also emerged, contributing to the refinement of detection systems by incorporating diverse sources of information and capturing intricate patterns.

The integration of multilayer algorithms within the data mining framework has shown promising results in minimizing false positives and false negatives, thus improving the overall reliability of fraud detection systems. Researchers have conducted extensive experiments on real-world credit card application datasets, validating the efficacy of these multilayer approaches in identifying suspicious activities indicative of identity theft.While existing literature highlights significant progress, there remains ample room for future research. The dynamic nature of fraud necessitates ongoing adaptation and innovation in detection techniques. Additionally, the incorporation of explainable AI and ethical considerations surrounding user privacy and data security are areas that warrant further exploration.In conclusion, the literature survey underscores the increasing importance of data mining techniques, particularly multilayer algorithms, in the detection of identity theft within credit card application forms. The surveyed studies collectively contribute to a deeper understanding of the challenges, advancements, and potential avenues for further research in this critical domain of cybersecurity and fraud prevention.

In 2005, Efstathios Kirkos et al. conducted a study focused on leveraging Data Mining (DM) classification techniques for detecting fraudulent financial statements. Their research explored factors associated with fraudulent financial statements and assessed the

effectiveness of Decision Trees, Neural Networks, and Bayesian Belief Networks in identifying such fraud. They used financial statement-derived ratios as input and compared the models in terms of performance, highlighting the model with the highest accuracy and underscoring the value of financial ratios in fraud detection.

In 2007, Dianmin Yue et al. proposed a comprehensive framework for the analysis of Fraudulent Statement of Financial Position (FSF) detection, addressing critical issues and setting directions for future research. In the same year, Clifton Phua et al. addressed limitations in non-data mining detection systems for credit application fraud, introducing a multilayered detection system that incorporated communal and spike detection techniques. These techniques improved detection capabilities, adaptivity, and quality data.This body of research contributes to the growing understanding of fraud detection methodologies, their effectiveness, and the need for adaptive, multifaceted approaches in combating evolving fraudulent activities.

In 2009, G. Apparao et al. emphasized the significance of fraud prevention and detection, noting that while prevention measures are essential, effective detection becomes crucial if preventive mechanisms fail. They explored data mining algorithms to extract relevant knowledge from vast datasets to detect fraudulent financial statements.

In 2010, Shiguo Wang et al. categorized, compared, and summarized data sets, algorithms, and performance metrics in automated accounting fraud detection. They highlighted the evolution from auditor data to encompassing factors like company governance and financial statement data.

In 2011, Tatsuya Minegishi et al. delved into classification learning through stream mining for fraud detection in credit card transactions. They introduced statistical criteria for a Very Fast Decision Tree learner to manage imbalanced distribution data streams.

In 2012, Sherly K.K et al. evaluated classification methods for fraud detection, demonstrating how advanced techniques can be combined for comprehensive fraud coverage with minimal false alarms.

In 2013, Alka Herenj and Susmita Mishra explored the application of CD (Communal Detection) and SD (Spike Detection) algorithms to bolster secure credit card transaction mechanisms. These algorithms were harnessed to create enhanced security layers, showcasing the

potential of such techniques in safeguarding credit card-based transactions from potential threats.

K. Vidhya and P. Dinesh Kumar, in 2013, emphasized the significance of the Spike tracing algorithm within data mining for detecting fraud, particularly when unique identifiers like passport numbers with biometric attributes were used. Their work shed light on the potential of specialized data mining techniques in identifying fraud patterns characterized by sudden spikes in data.

In 2017, John O. Awoyemi et al. contributed to the field by employing machine learning techniques, including Hybrid Sampling, Naïve Bayes Classifier, and K-Nearest Neighbour Classifier, to address the challenge of identifying credit card fraud. Their research highlighted the efficacy of machine learning algorithms in analyzing transaction patterns and data to accurately detect fraudulent activities.

Aditya Asgaonkar and Bhaskar Krishnamachari delved into the realm of blockchain-based solutions by focusing on the integration of simple cryptographic primitives. Their study revolved around the development of a blockchain-driven system that employed cryptographic building blocks, showcasing the potential of such a framework in enhancing security and privacy aspects.

In 2019, Wenbo Wang et al. directed their attention toward the application of blockchain technology in a Byzantine environment to tackle the challenge of detecting identity crime. By harnessing the decentralized and tamper-resistant nature of blockchain, their work aimed to enhance the accuracy and security of identity crime detection methods within a Byzantine context.

In 2021, E.M.S.W. Balagolla et al. presented a novel approach to combat credit card fraud utilizing the B-Box.com environment, which operates on the principles of blockchain technology. This environment was harnessed to create a robust and secure platform for thwarting credit card fraud incidents, leveraging the inherent strengths of blockchain in ensuring transparency and immutability of transaction records.

The research contributions highlighted above collectively underscore the growing trend of utilizing advanced technologies such as blockchain and machine learning, as well as specialized data mining algorithms, to address the pressing issue of fraud detection in various domains, particularly credit card transactions.

Working and Architectural daigram :

The proposed system employs a novel approach involving two distinctive layers, termed Communal Tracing (CT) and Spike Tracing (ST), aimed at fortifying the security of credit card transactions within application processes. The uniqueness of this research resides in the strategic integration of these dual data-mining layers, contributing to the enhanced detection of fraudulent activities across various dimensions.

A. Communal Tracing:

The Communal Tracing layer introduces a whitelist-driven methodology, employing a predefined set of attributes to discern genuine social connections and reduce suspicion scores, thereby ensuring resilience against tampering attempts involving synthetic social relationships [1]. The CT algorithm facilitates the comparison of all linkages against the whitelist, facilitating the identification of communal associations and a subsequent reduction in their linkage scores. However, a potential limitation of CT lies in its attribute threshold, mandating at least three matching values within the dataset for detection, thus missing instances where crucial values are duplicated by malicious entities. CT further accounts for attribute weights and undertakes comparisons with prior applications within a moving window to compute the score of the current application. At the conclusion of each Mini-discrete data stream, a random parameter's value is systematically adjusted to maintain equilibrium between efficiency and effectiveness, ultimately generating a refreshed whitelist grounded in the current linkages.

The iterative steps encompassed by the CT algorithm are as follows:

i) Evaluate each application value against a record of preceding application values to uncover linkages.
ii) Scrutinize each application's link in relation to the whitelist, enabling the identification of communal relationships and subsequent reduction of their Link scores.
iii) Aggregate scores from prior applications with the current application's score, utilizing link information and previous application scores to determine the present application's score.
iv) Modify the value of a randomly selected parameter to ensure a balance between efficiency and effectiveness, consequently creating a new whitelist based on the prevailing Mini-discrete stream linkages.

Communal tracing Algorithm steps :

1. **Attribute and Linkage Score Calculation:**
   - For each attribute a in the application and each linkage l in the moving window, we compute a score $S_{a,l}$ based on how similar the attribute value a is to the linkage value l.
2. **CT Suspicion Score Calculation:**
   - The CT suspicion score S_{CT} for the current application is determined by adding up all the scores $S_{a,l}$ across all attributes and linkages:
     $S_{CT} = \quad _a \quad _l S_{a,l}$
3. **Attribute Weight Adjustment:**
   - Attribute weights W_a are applied to fine-tune the impact of each attribute on the CT suspicion score:
     $S_{CT} = \quad _a W_a \cdot \quad _l S_{a,l}$
4. **Attribute Weight Updates:**
   - At the end of each Mini-discrete data stream, the algorithm modifies the attribute weights W_a using a function F that considers both effectiveness and efficiency:
     $W_a^{\text{new}} = F(W_a^{\text{old}})$

In essence, the CT algorithm calculates a suspicion score for each application by looking at how attributes match with linkages. It uses attribute weights to adjust the importance of each attribute and periodically updates these weights to maintain a balance between effectively detecting genuine relationships and efficient processing.

By combining the Communal Tracing layer with the subsequent Spike Tracing layer, this research endeavors to establish a more comprehensive and adaptive mechanism for detecting fraudulent activities within credit card application processes.

Diverging from the approach of Communal Tracing (CT), Spike Tracing operates on a different premise by focusing on the identification of spikes, a strategy aimed at elevating the suspicion score while rendering the attributes resilient to probing attempts. This unique strategy is devised to curtail the chances of malevolent actors accessing the attributes essential for computing the Spike Tracing (ST) score. Employing an attribute-oriented framework, ST exhibits a selective nature, opting for attributes that are neither excessively sparse nor overly dense. It calculates the ST suspicion score, periodically purging superfluous attributes to enhance efficiency.

B. Spike Tracing:

The ST algorithm involves the following distinctive steps:

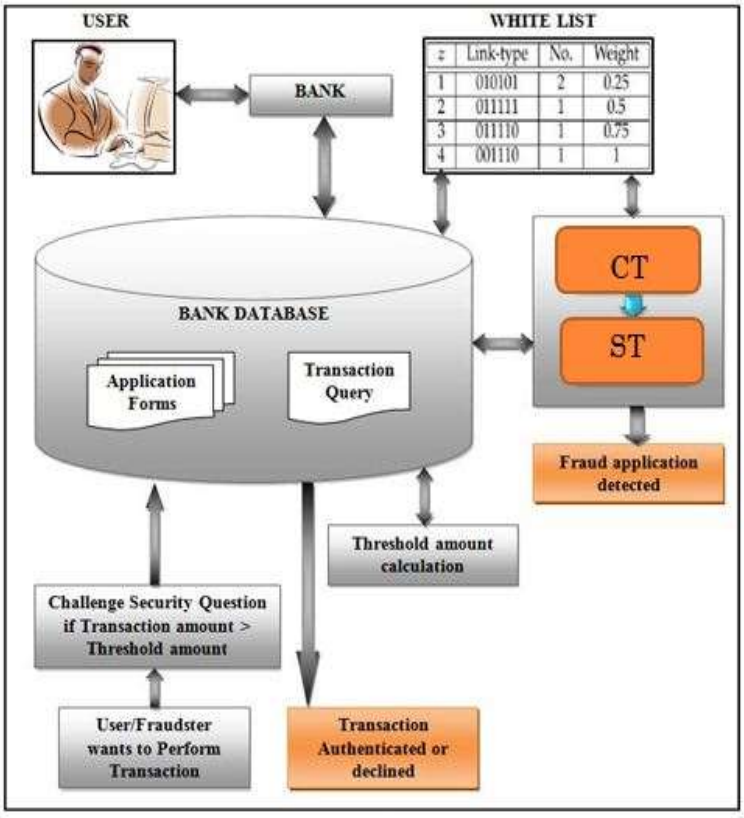
i) Sequentially match each application value against the roster of preceding application values.
ii) Integrate an array of steps to pinpoint spikes, ultimately culminating in the computation of the present application's score.
iii) Factor in attribute weights to formulate the application's score.

iv) Discern the pivotal attributes governing the ST suspicion score computation, subsequently refining the attribute weights in alignment with the end of each Mini-discrete data stream.

By juxtaposing the insights derived from Spike Tracing with the preceding Communal Tracing methodology, this study aspires to furnish a holistic and adaptable framework for the detection of fraudulent activities within credit card application protocols.

Spike Tracing Algorithm steps :

1. **Spike Identification and Score Calculation:**
   - For each attribute a in the application and each prior application value v in the moving window, we determine if the attribute value a is a spike by comparing it with the values in the window. If it's a spike, we calculate a spike score $S_{a,v}$ based on the deviation from the average value in the window.
2. **ST Suspicion Score Calculation:**
   - The ST suspicion score S_{ST} for the current application is calculated by adding up all the spike scores $S_{a,v}$ across all attributes and prior values:
     $S_{ST} = \quad _{a} \quad _{v} S_{a,v}$
3. **Attribute Selection and Filtering:**
   - ST adopts an attribute-oriented approach by selecting attributes that are moderately dense and not too sparse. These attributes are used to calculate the ST suspicion score. Redundant attributes are periodically filtered out to maintain efficiency.
4. **Adjusting Attribute Weights:**
   - The algorithm adjusts the attribute weights W_a for the ST suspicion score calculation. These weights reflect the significance of each attribute in identifying spikes.



z	Link-type	No.	Weight
1	010101	2	0.25
2	011111	1	0.5
3	011110	1	0.75
4	001110	1	1

Figure1.1. : Syetm Architectural diagram for credit card application form fraud detection system

The system architecture encompasses the subsequent components:
An intuitive graphical interface that facilitates users in entering credit card application details.The system acquires and stores the user's provided data.A comparison of linkage types is executed between the incoming application and all pre-existing applications within the bank's database. This linkage classification is represented by a binary string, where "1" signifies matched attributes and "0" denotes unmatched data.Subsequently, the system generates an initial white list, constituting a validated application inventory, the specific linkage type, the count of applications associated with that linkage type, and its corresponding weight.The procedure of

Communal Tracing entails the following sequential steps:

a) The system undertakes a meticulous comparison between a novel application and the records present within the white list.
b) Within the Communal Tracing (CT) layer, the system proficiently identifies resemblances among applications, ultimately contributing to the detection process.
c) When the new application displays a match in four or more fields with the application from the white list, Communal Tracing (CT) allocates a decreased level of suspicion to the transaction.
d) In cases where such a match does not occur, the new application is integrated into the white list, leading to its subsequent update.
e) The Suspicious Transaction (ST) layer receives the suspicion score assigned to the newly submitted application as its input.

The progression of Spike Tracing encompasses these sequential steps:

a) Within the ST layer, a meticulous evaluation of matched fields is conducted, with special attention given to unique identification attributes, which are accorded the highest priority.
b) Should the evaluation reveal the presence of unique IDs, the suspicion score undergoes elevation, prompting the system to label the application as suspicious and ultimately leading to its rejection.
c) If no matching unique IDs are identified, the application form becomes an addition to the white list, subsequently prompting an update of the list.

Additionally, the system calculates the transaction amount threshold grounded on the user's historical transactions. This threshold value is ascertained by the cumulative sum of all preceding transactions.

Results:

In an era characterized by rapid e-commerce expansion, combatting fraud has assumed paramount significance. Fraud tracing remains in a perpetual state of evolution, with fraudsters continuously devising novel tactics. Traditionally, credit card fraud detection has leaned on business rules, scorecards, and established fraud matching methods, all fraught with limitations. Conventional approaches confine their scope to post-fraud identification. In response, the present system harnesses data mining techniques to proactively thwart credit card fraud. This paradigm shift from reactive to preemptive aims to obstruct fraudsters from gaining access to credit cards in the initial stages. Leveraging an adaptive economic environment, the system dynamically selects data mining techniques optimally suited for fraud tracing, with the overarching objective of refining accuracy, speed, and cost-effectiveness.The generation of link types via binary strings emerges post a meticulous comparison between attributes of the ongoing application and those within the white list. This linkage classification is accompanied by the generation of application form attribute weights and corresponding suspicious scores.

Validation of credit card application forms rests on the system's capacity to discern acceptance or rejection. Strengthening the security facet for online transactions, the system employs challenge security questions to authenticate legitimate individuals.

Operationalizing the system relies on a synthetic data set comprising 50,000 credit applications, accessible at https://sites.google.com/site/cliftonphua/communalfraud-scoring-data.zip. From this dataset, 19 pivotal identity attributes are selected for processing, out of the 30 attributes originally present. User-initiated credit card applications, coursed through an online web portal, constitute real-time system inputs. These applications undergo scrutiny, involving a comparative analysis against the synthetic data set's applications. The resultant validated entries contribute to the construction of a white list. Subsequently, the application receives a CT suspicious score via communal detection algorithm, and a ST suspicious score via spike detection algorithm. These scores are then amalgamated to furnish a unified evaluation. Furthermore, ST's iterative updates encompass the adjustment of CT attribute weights, further reinforcing the system's resilience and adaptability.

A key feature of the system entails the dynamic updating of the CT and ST layers. This practice is pivotal to thwarting potential subsequent attacks by fraudsters. The end result is a real-time credit application fraud tracing mechanism founded upon the bedrock of data mining layers. The essence of this research endeavors to establish a

methodical real-time search for patterns, consequently safeguarding credit applications throughout transactions.

Integral to this system are core principles, including:

1. Resilience: Orchestrating multilayer protection mechanisms to ensure comprehensive safeguarding.
2. Adaptivity: Ensuring readiness to respond to the ever-evolving landscape of fraudulent and legal behavior.
3. Data Quality: Enabling real-time rectification of data discrepancies to enhance overall accuracy.

Thus, the initiative stands as a comprehensive endeavor to fortify credit application security by embedding cutting-edge data mining strategies, reflecting a commitment to resilient, adaptive, and high-quality fraud tracing methodologies.

Rec_id	First Name	Last Name	Address	City	State	Postcode	MobileNo	Adhar No	PAN_id	DOB	Status
1	kale	noyce	bural court	forbes	vic	423075	7532950055	123456789101	AMZGT1000A	11/10/1947	Accepted
2	bella	chemny	howie court	nambour	vic	422540	7558336354	123456789102	BNAHU1001B	29/01/1931	Accepted
3	charlotte	bullock	bungaree crescent	wagoora	qld	422154	7570610247	123456789103	COBIV1002C	10/10/1982	Accepted
4	esme	jardine	kirby place	woodville north	nsw	423233	7559190277	123456789104	DPCJW1003D	30/10/1949	Accepted

Figure 1.2 Dataset of accepted list

6	thomas	matthews	maranoa street	marayong	nsw	423104	7573884029	123456789107	GSFMZ1006G	27/12/1932	Pending
7	anurag	sangale	bungaree crescent	wagoora	qld	422154	8806323532	123456789103	ABCDE1234F	22/12/1990	Pending

Figure 1.3 Input Dataset

Link-type	Count	Weight
0000100101	1	0.11
0000010101	1	0.22
0000010101	1	0.33
0000010101	1	0.44
0000000101	1	0.55
0000000101	1	0.66
0000100101	1	0.77
0000110101	1	0.88
0011010100	1	1

Figure 1.4 White List

The depicted illustration in Figure 1.4 provides an exemplar of the generated white-list, stemming from the credit applications delineated in Figure 1.2 and Figure 1.3. The resultant outcome of the Spike detection algorithm yields the ST suspicious score. Both the CT and ST scores are amalgamated to yield a unified score. It's noteworthy that the ST mechanism also contributes to the enhancement of CT attribute weights.The dataset pertains to a collection of approved credit card applications. Specifically, it encompasses a subset of five entries categorized as "accepted." These records exhibit a total of 12 attributes, including two distinct elements: Adhar card number and PAN ID, both associated with the "accepted" status.Record no. 6 and 7 are the input dataset to the system. Here the status of the records is in pending status.The figure 1.4 shows the White-List constructed by the CT algorithm as a result during processing the Input dataset.

6	thomas	matthews	maranoa street	marayong	nsw	423104	7573884029	123456789107	GSFMZ1006G	27/12/1932	Accepted
7	anurag	sangale	bungaree crescent	wagoora	qld	422154	8806323532	123456789103	ABCDE1234F	22/12/1990	Rejected

Figure 1.5 Processed Applications

Upon the utilization of the CT and ST algorithms, the system undertakes computations to derive the link type and attribute weight. Subsequently, following the effective execution of these procedures, the status of the record undergoes a transition from pending to either accepted or rejected.

Conclusion:

The primary objective of this project is to construct a multi-tiered fraud detection framework tailored to identify fraudulent activities within credit applications, leveraging advanced data mining techniques, notably the Communal Tracing (CT) and Spike Tracing (ST) layers. These interconnected layers collaborate to ensure secure real-time transactions by discerning instances of duplicated fraudulent actions as well as authentic social connections. The regular updates to both the CT and ST layers serve the purpose of preempting potential further attacks by fraudsters. Through the development and assessment of a real-time credit application fraud tracing system anchored in data mining strata, this research aims to execute a methodical pattern search in real-time, bolstering the security of credit applications throughout transactions.

A central objective of this study revolves around the principled execution of real-time pattern searches, actively safeguarding credit applications in transactional contexts. Guided by principles such as resilience (implementing multiple protective layers), adaptivity (addressing evolving fraudulent and legal behavior), and data quality (real-time rectification of inaccuracies), this system underscores the pursuit of comprehensive, adaptable, and high-quality fraud detection methodologies.

References :

[1] E.M.S.W. Balagolla et al., "B-Box.com: Blockchain-based secure credit card fraud prevention," in Proceedings of the 2021 IEEE 16th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), pp. 63-68, 2021.

[2] W. Wang et al., "A blockchain-based approach for identity crime detection in Byzantine environments," in Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), pp. 570-576, 2019.

[3] Asgaonkar and B. Krishnamachari, "A blockchain-based approach for securing credit card transactions," in Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), pp. 682-689, 2019.

[4] K. Vidhya and P. D. Kumar, "Fraud detection in credit card transactions using spike tracing algorithm," in Proceedings of the 2013 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1-5, 2013.

[5] Herenj and S. Mishra, "Communal detection and spike detection algorithms for secure credit card transaction mechanisms," in Proceedings of the 2013 IEEE International Conference on Data Mining and Advanced Computing (SAPIENCE), pp. 339-344, 2013.

[6] S. K. K et al., "Comparative analysis of classification algorithms for fraud detection," in Proceedings of the 2012 IEEE International Conference on Data Science and Data Intensive Systems (DSDIS), pp. 327-332, 2012.

[7] J. O. Awoyemi et al., "Anomaly-based detection of credit card fraud: A machine learning approach," International Journal of Data Analysis Techniques and Strategies, vol. 9, no. 3, pp. 297-314, 2017.

[8] S. Wang, K. Zhao, and J. Zhou, "A comprehensive review of data mining-based fraud detection research," IETE Technical Review, vol. 27, no. 5, pp. 367-385, 2010.

[9] G. Apparao, P. S. Kumar, and P. R. Prasad, "Fraudulent financial statement detection in the advanced big data environment," Procedia Computer Science, vol. 93, pp. 60-67, 2016.

[10] D. Yue, J. Wu, and J. Huang, "Fraudulent statement of financial position detection: A comprehensive framework," Decision Support Systems, vol. 43, no. 1, pp. 272-282, 2007.

[11] E. Kirkos, C. Spathis, and Y. Manolopoulos, "Data mining techniques for the detection of fraudulent financial statements," Expert Systems with Applications, vol. 32, no. 4, pp. 995-1003, 2007.