International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Online Fraudulence Detection Based on Decision Support System in Digital Banking

Madasamy Raja. G[1], Amudha. G[2], G. Gomathy[3], P. Kowsalya[4], R. Salini[5]

Submitted: 15/12/2023 **Revised:** 27/01/2024 **Accepted:** 06/02/2024

Abstract: The widespread use of online banking operations is anticipated to climb additionally as applications for digital banking progress. An unforeseen impact of this pattern is a surge in fraud attempts. On the other hand, the scientific research on spotting online banking scams is astonishingly thin. Our proposed solution is an attention-based structure that can be utilized to differentiate between truthful and bogus online banking transactions. In this article, a Decision Support System based on Machine Learning is proposed that automatically allocates a risk factor to each payment produced via a mobile device or online financial system. Since there is an enormous rise in the total amount of people using the internet, this suggested approach will be more effective in hindering unidentified hazards and malicious activity. The framework of the claimed method is structured: In advance of supplying a risk factor for activities that were not flagged as irregularities in the preceding phase, a controlled machine learning section is executed to recognize unusual behaviors or purchases that were mistakenly labeled. The final results of the simulation reveal that the concept of intelligent decision-making demonstrated in this paper has some real-world applications.

Keywords: *DSS, online fraud detection, safe transactions, Banksealer architecture*

1. Introduction

Over 60 percent of citizens in various nations engage with the internet or mobile phones to purchase financial items, making digital banking a common outlet for transactions in money and items bought. However phone banking scam arises when an attacker receives fake credentials to the victim's mobile banking account, online banking scam arises when an intruder gains access to a person's online bank account and transactions money from it. Every year, financial crime produces immense damage worldwide. In the UK, for instance, the total loss from fraudulent checks, payment cards, and electronic banking was 768.8 million. It was practical to halt fraud for an entire amount of 1.38 billion at the same time. Nevertheless, recognizing that unwarranted hindering of financial services is highly irritating to consumers and could potentially increase the rate of turnover challenges the safeguarding of fraudulent transactions. As a result, before determining to stop an electronic transaction, safeguarding mechanisms necessarily require human assistance [1].

A notion of the part of computers in reaching choices is illustrated by Decision Support Systems (DSS). Investigators, professionals and administrators who express concern that the disciplines of management science and management information systems have irrationally restricted their focus have dedicated themselves to promoting around this term. Identical to several encouraging calls, the expression lacks a clear description. Some writers comprehend DSS as simply interactive systems envisioned for leadership use. For certain people, it's primarily about their assistance than the system. They emphasize recognizing and improving the decision-making process; any suitable and easily accessible innovations in technology are then utilized to design a DSS. While some researchers see DSS as a branch of management science techniques other individuals see it as a related branch of MIS [2].

As demonstrated in Figure 1.1, a DSS's primary components are organizing data, model supervisors, user interface, knowledge administration, and users. A DSS is a flexible instrument that makes it effortless for decision-makers to evaluate and interpret reasoning models and oversee data in a manner to solve complicated non-repetitive and informal decision-making duties. Decision-makers utilize the interface and management segments for using the system, and they draw numerous types of data and information concerning the framework of databases under their demands [3].

[1]*Professor, Department of Information Technology,
Paavai Engineering College, Namakkal, Tamilnadu,
Email: drgmraja@gmail.com
ORCID: 0000-0002-8410-4733*
[2]*Professor, Computer Science and Business Systems,
R.M.D. Engineering College, Chennai
Email: gav.csbs@rmd.ac.in
ORCID: 0000-0002-2583-6475*
[3]*HOD, EEE Department, Jaya Engineering College, Chennai-24,
Thiruvallur District, Tamil Nadu
Email: gomathypaul@gmail.com
ORCID: 0009-0007-1367-0715*
[4]*Assistant Professor, Department of ECE,
Madanapalle Institute of Technology & Science,
Madanapalle, A.P
Email: kowsipremmdu@gmail.com
ORCID: 0009-0006-0581-9965*
[5]*Assistant professor, Department of CSE,
Panimalar Engineering College, Chennai
Email: shalinirajendran@gmail.com
ORCID: 0000-0001-7266-3389*

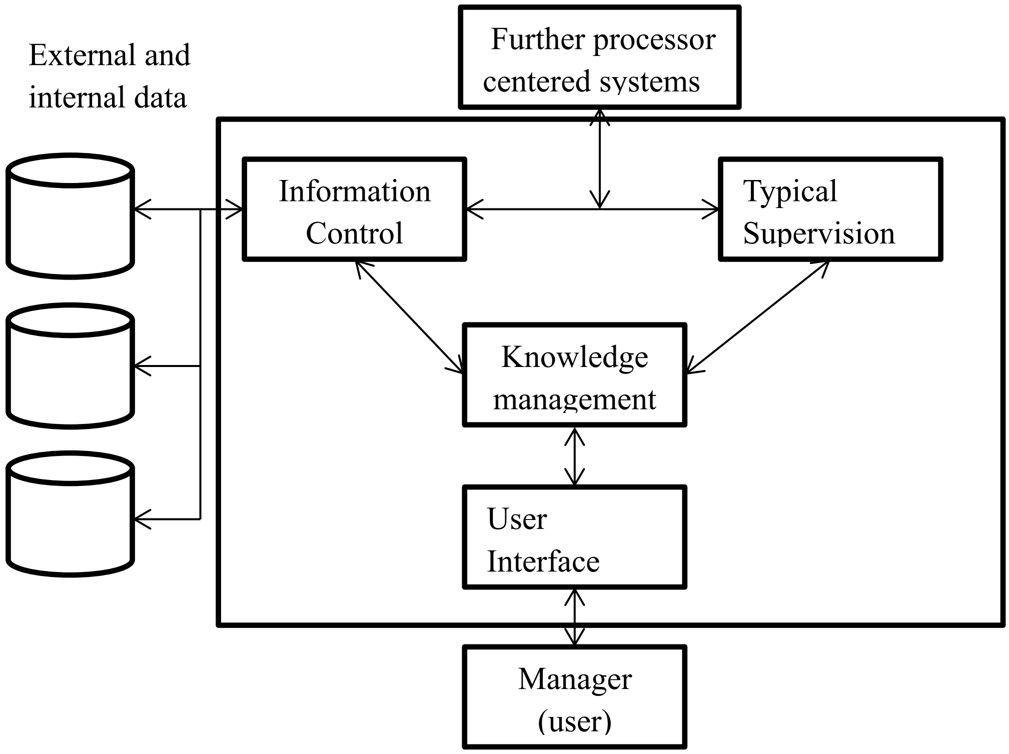

Fig. 1.1. DSS components

With Banksealer we proposed a successful online financial transactions selection and scams analysis system. Particularly Banksealer swiftly rates irregularities and thefts in payments involving debit cards, prepaid mobile devices, and money transfers. Over an education phase, it develops a localized, international, and temporal profile for each individual. Prototypes of individual profiles that go beyond customer habits facilitate easy analysis of unusual new purchase activity. Based on their transaction attributes, users are categorized collectively in their global persona. The objective of the temporal profile is to illustrate actions using attributes that evolve over time. Banksealer is also in control of user profile inadequate training [4].

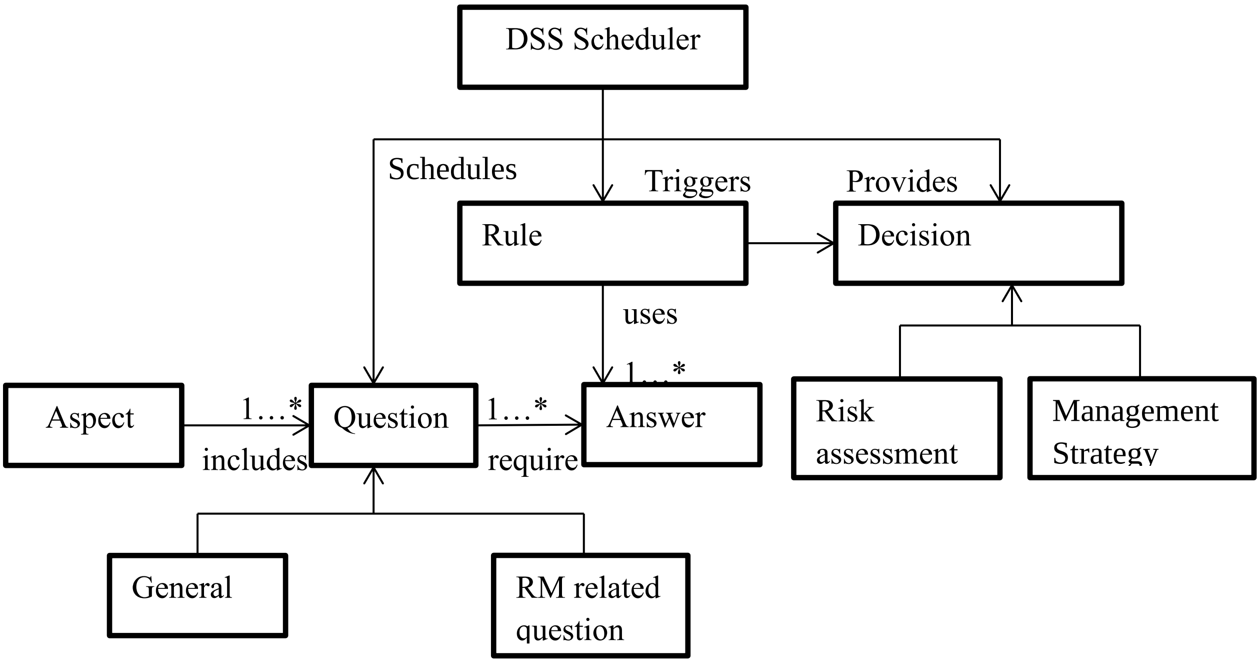

Fig. 1.2. Decision support model

The basic approaches and decision support model for excellence identification are laid out in Figure 1.2. More specifically when it pertains to finances, problems can grow incredibly convoluted and haphazard. The enormously dynamic, rapidly changing data sets present, the incredibly proficient computational financial frameworks in use, and the prospect of disastrous losses all play an integral role in increasing the importance of DSS in the finance sector. The financial sector vulnerability has an omnipresent impact throughout finance; it permits the operation of the decisions beneath the whole thing from expenditures techniques, mortgages, and portfolio positions to interest prices, asset price tags, regulatory compliance, and capitalization rates. The high relevance of DSS in this domain is attributed to the importance of financial danger in financial decision-making and the complicated nature of its inspection [5].

A spanning overview of each portion of this skilled dedication is offered in this follow-up article. The first portion renders clearly that the inquiry's initial dedication will be associated to DSS. Section 2 illustrates the distinctive characteristics of deploying data mining for measuring student fraudulent identification in the banking sector. To make sure that learning statistical analysis is completed by employing a unique procedure, this third section assesses. The aspects of the system task, statistical examination, easy to comprehend theoretical framework, and graph-based conduct are given special consideration. In Section 4, a multitude of peculiar visualizations and graphs encourage decision-making. Section 5 incorporates the results-oriented conclusion for this proposed method.

2. Related Works

Mukhopadhyay, A., Chatterjee, S et. al [6] The Bayesian Decision Support System (BDSS) was developed for evaluating IT risk through statistical tools. The data submitted to the BDSS were (i) resource recognition and ruin impact organizing, (ii) threat analysis and susceptible mapping, (iii) stimulation dispersion, and the occasion rate. The outcomes of the BDSS embrace (i) a danger distribution for every threat, (ii) a technical analysis with extensive information on the safety features to be utilized, and (iii) the feasibility of the safety measures to be accepted to mitigate the vulnerability of the network.

Naseem, A., Shah, S. T. H. et. al [7] Based on immediate limitations and changing circumstances, the real-time DSS (RDSS) creates output swiftly It involves managing intricate circumstances, multiple tasks, and meta-modeling. It is an engaged software-based framework produced to aid decision-makers in acquiring essential information by bringing together documents, personal knowledge, and unstructured information with frameworks to assist them in detecting and fixing challenges. It fosters the generation of ideal remedies.

Mecati, M., Cannavò, F. E. et. al [8] For the purpose of helping to label datasets as well as recognize possible dangers of discriminatory revenue when employed in decision-making or DSS, the researchers offer an analytical and functional framework. As an outcome, the aim is to collect and organize dataset metadata to support software developers in grasping potential hazards of inequality.

Ngai, E. W., & Wat, F. K. T. et. al [9] The splitting of labor that occurs between a data center and the customers that access it is sometimes referred to as the client-server interaction. A client-server framework with a two-tiered structure is the FDSS. It is a front-end technique that collaborates with users of the web for gathering service inquiries and displaying final results on the customer side. It is a back-end system that travels a physical database for handling information and an ambiguous risk evaluation on the server side. Promoting unimportant programs with low business transaction loads, like managerial apps or DSS, is an optimal fit for a two-tiered design.

Carminati, M., Caron, R. et. al [10] We offer BankSealer, an excellent semisupervised online banking fraud assessment and decision support framework, in this article. When it comes to bank transfer deals, prepaid phone activities, and debit card interactions, BankSealer effortlessly ranks frauds and irregularities. It establishes a regional, international, and spatial profile for all users during the learning phase.

Tyugu, E. et. al [11] Broad understanding application is needed for decision making, and one of cyber defense's remaining problems are clever decision support. It can be submitted straight to decision support, like anything in cyberspace, financial matters, or healthcare diagnosis. Expert solutions possess an extensive selection of measurements and potential, from dense technical testing equipment to immensely complex hybrid structures for handling complex problems.

Sharma, A., & Panigrahi, P. K. et. al [12] The primary objective is to detect fraudulent accounting records employing a hybrid decision-support framework that uses building variant procedure. Some research projects target to determine financial fraud in a particular country by applying the basic model of logistic regression. Several recent investigations in the arena of financial fraud detection contrast the success rate of two or more data mining strategies or use an integrated approach.

3. Methods and Materials

Devices facilitate formulating choices for threat assessment and deciding on a permitted management strategy. A DSS is developed by taking into account the already launched DSM and the output of SLR. There are multiple steps in the decision-making process, such as an assortment of questions, reactions, and triggering conditions. It is an online tool that businesses can use for free. It evolved with SQL server and the MVC.Net arrangement, employing Entity Framework. Javascript and JQuery are utilized on the customer side. Both decision-makers and decision-planners may use this tool. The application designed for the decision-making process can be employed and customized by decision designers. Option-making executives, such as project leaders, can pick and use previously established DSS to support them in risk evaluation and administration plan selection. The Knowledge Base (KB), Decision Support Engine (DSE), and Graphical User Interface (GUI) are the three sections of the DSS for the risk evaluation and management approach, depicted in Figure 3.1. Database and decision support components are expressed by the KB of DSS and DSE, accordingly. Knowledge base source encompasses the outcome of the SLR. It has four fundamental parameters, 49 attributes, and the 524 dangers that go together with them, on top of their order of importance and supplementary management strategies. The decision maker can use further details or regulations established from the SLR to reinforce their logic while using the DSE. Users can communicate with the KBDSS for DSD risk administration via the GUI. It additionally includes fundamental information concerning the upkeep of the system. Radar charts and bar graphs are the analysis and mental imagery outcomes that the GUI will exhibit.

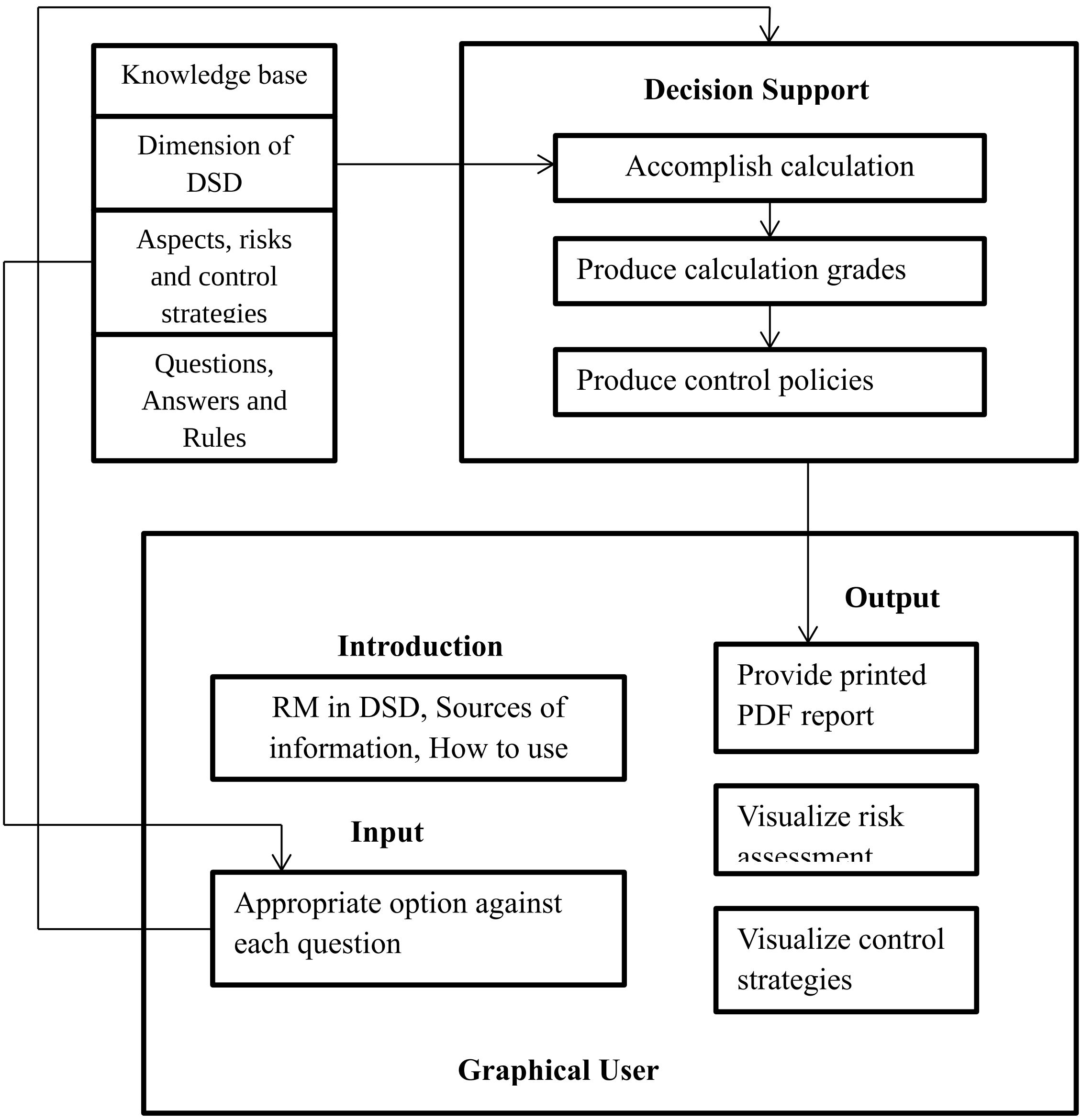
Knowledge base
Dimension of DSD
Aspects, risks and control strategies
Questions, Answers and Rules
Decision Support
Accomplish calculation
Produce calculation grades
Produce control policies
Output
Introduction
RM in DSD, Sources of information, How to use
Provide printed PDF report
Input
Visualize risk assessment
Appropriate option against each question
Visualize control strategies
Graphical User

Fig. 3.1. Architecture of DSS

3.1 Hazard Recognition And Organizing By Parts

The probability of threat and the DSD's achievable defenses were addressed in previous parts. Choosing before identified risks regularly follows the determination of specific challenges. The decision-maker will discover the relative position of options with the assistance of making decisions. It also supports project scheduling and allocating funds to each project's tasks for them or the project manager. The Analytic Hierarchical Process (AHP) strategy is a commonly employed method for assessing the relative value of multiple risk factors. AHP is implemented to evaluate the alternatives to receive an organized set of requirements, and then choose the most beneficial choice from the list of variants. It has proven efficient in a wide range of domains, incorporating risk evaluations for Nano Carbon goods, agricultural water management scrutiny, large manufacturing business threat prioritization, industrial machinery security measure hiring, stakeholder quality characteristic estimation and setting goals, etc.

In order to avoid breakdown, this research analyzes probability factors connected with DSD employing the AHP strategy. The recommended way for utilizing AHP is executed. Following is a straightforward summary of it.

Step 1: List and explain the parameters that are measured or placed in tandem with their substitutes.

Step 2: A pairwise comparison of each aspect will be employed to establish the overall significance of each factor. An m x m matrix, M (m i,j), with i, j = 1, 2, 3,...n, embodies the phase's output.

$$N = \begin{bmatrix} n_{11} & n_{12} & n_{1m} \\ n_{21} & n_{22} & n_{2m} \\ n_{n1} & n_{n2} & n_{nm} \end{bmatrix} \qquad (1)$$

Where $n_{j,k} > 0$ and $n_{j,k} = 1/(\ n_{j,k})$

When i and j are identical, then the two factors have a corresponding significance, i.e., $n_{j,k} = n_{j,k} \cdot = 1$.

The proportional rating of $n_{j,k}$pursuant to the phonological scale is presented in Table 3.

Step 3: Utilize the pairwise comparison matrix, M, to figure out the total weight at the end. Regulate the quantities that are found after processing.

$$X = (x'1, x'2, x'3, \dots x'o)^U \qquad (2)$$

Every matrix's load is computed by splitting its index readings by the aggregate of its column readings. Add every factor collectively throughout the computation, and then break down the entire amount by the number of components in those rows.

$$x'j = \sum_{k=0} \left(\frac{n_{jk}}{\sum_j n_{jk}}\right) \qquad (3)$$

To ensure the uniformity of comparison between pairs, the consistency index is computed as

$$CI = \frac{\vartheta_{max-o}}{o-1} \qquad (4)$$

The Eigenvalue's highest possible value is portrayed by λmax. It is found based on the next equation (5), which

$$\vartheta_{max} = \frac{1}{o}\sum_{j=1}^{o}\frac{(Bx')_j}{x'j} \qquad (5)$$

The purpose of the pairwise evaluation matrix, M, is to establish the objective precedence across different requirements. Following is a pairwise comparison of an overall vector of an aspect number of sites (Table 1). Matrix M is generated by incorporating the findings of the SLR. The main goal of various elements was set about the multilingual scale by reiterating things right through surveys and discussing users and industry specialists. To obtain importance from professionals, no well-organized survey was put in place though [13].

Table 1. AHP matrix

	PS	C&C	RA	M	DM	DD
PS	2	1/4	3	3	1/3	2
C&C	4	2	3	3	3	4
RA	¾	¾	2	2	3	2
M	¾	¾	2	2	4	5
DM	5	¾	¾	2/3	2	3
DD	2	¼	2	1/3	1/4	2

4. Implementation and Results

4.1 Evaluating Consequences

Each of the financial dataset undergoes the exact same technique, which starts out with conversion of data and finishes with system administration. Alternative account numbers that were not supplied insufficient behaviour may have been the basis of dubious conduct. The technique catches those interactions as it meets the conditions that were given within the methodology itself. All of the banking dataset is validated using the standard parameter settings. Table 2 is the standard configurations required to analyze the system.

Table 2. Attributes used for evaluation

Constraint designation	**Limit Expanse**
Period:	8 days
Modification from mean:	4 σ
Variance from Threshold:	76 quantile

Each of the financial dataset has a distinctive treatment result depending on how numerous operational logs are in it and how the settings are set up. However, this won't suffer from an influence on the procedure's precision simply because it will only recognize behavioral categories that match the fraud parameters. The scam indicators are customizable and can be altered by the operator on the Parameter Setup Page. As a result, the outcome will be highly reliant on the user-configured factor. In Scenario 2, by implementing two phases of screening, the algorithm was able to pick up suspicious transactions that are not observed within the primary layer, resulting in a further legitimate finding. Additional transactions which satisfy the fraud parameters are additionally read by the system. As a outcome, prevailing financial records without any freshly discovered unusual transactions stored in them are also accessible to spot unusual behaviour with the same methodology. Following preparation, the end result will be revealed on the Result Summary Page, where an individual can read each individual account number in additional information. The customer will gain the power to modify the Safety Level of the transaction categories on the Customer Detail Page. This grade is directly proportional to the Risk Level of the designated account number [14].

4.2 Implementation of Banksealer Architecture

The key features of BankSealer, an extensive structure to uncover fraud and irregularities in electronic banking that accumulates pertinent information for every customer and transaction, are dealt with in this subsection. Our technique's goal is to function as a decision support tool which assists bank analysts reveal frauds faster and more precisely by using three kinds of profiles that portray users of the online banking utilization: local, global, and temporal. These personas are established amid the training period. A list of monetary transactions is the input source for the learning stages, as shown in Figure 4.1. According to the form of model being built, each category of profile chooses a unique collection of demographic information from the trade parameters. After the client profiles are developed, BankSealer analyses any fresh transactions and ranks them relying on the anomaly score and foreseeable fraud risk. It performs under both semi-supervised and unsupervised hypotheses. With regards to the grasped profiles, the abnormality score determines the statistical certainty that an operation is counterfeit. Transactions are categorized based on both their total amount and irregularity score of potential fraud.

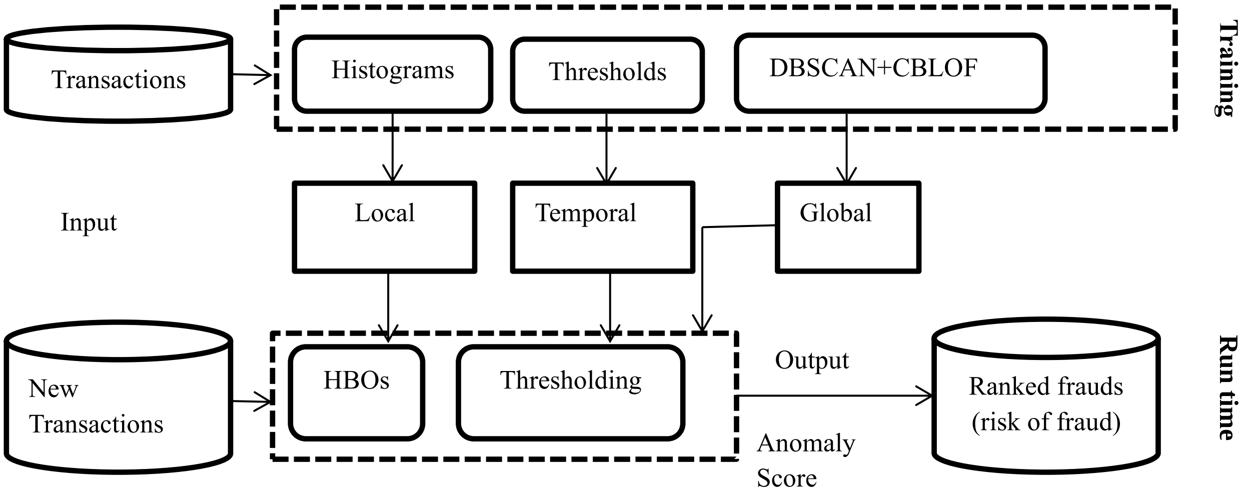

Fig. 4.1. Banksealer architecture

Instruction and Feature Withdrawal: The metrics of every variable explained in Table 1 are the attributes. Using uni-variate histograms and we calculate each feature's marginal dispersion during training. For the purpose of enhancing the comprehensibility of the visuals and to decrease spatial intricacy, we neglect to take feature relationship into account. Scientists readily comprehend uni-variate histograms and fully comprehend normal behavior by barely watching at the profile. Additionally, they render it easier for estimating an unusual result as an aggregate of each feature's investments, providing a clear rationale for the anomaly score that gets obtained. In the scenario of categorical traits (like IP and CC), we count the number of occasions every classification arises. We use periodic binning for numerical parameters (such as timestamps and amounts) and measure the quantity of instances that fall inside every bin. Subsequently we figure out the relative occurrence and evaluate the attributes' marginal distribution.

Our assessment intended to determine BankSealer's efficacy and computational resource needs in precisely identifying bogus transactions that have never been observed earlier. We achieved yet another hypothetical inspection of our system implementing mixed fraudulent situations on a wider set of data in order to verify its feasibility factually. We also go into even more detail about our system's reliability.

4.3 Dataset portrayal and scam situations

As a result BankSealer creates fresh information like any other alternate unsupervised analysis tool, evaluating it is extremely hard.

To further improve our testing datasets with genuine thefts based on incidents of fraud that mimic the frequent actual attacks perpetrated against online banking consumers, we thus count on the knowledge of domain specialists (bank operators). We emphasize on the most important and challenging fraud schemes of today, which are powered by phishing or banking Trojans (like Zeus and Citadel). The quantities for each dataset and scenario are displayed in Table 3.

Table 3. Amount transferred for each data set and scenario

Fraud Scenario		**Amount transferred (€)**		
		Bank transfers	Phone recharges	Prepaid cards
Data stealing		11,000-51,000	251-256	860-2,000
Transaction hijacking		11,000-51,000	251-256	860-2,000
Stealthy fraud	Very low amount	60-110	6-20	60-200
	low amount	200-600	11-26	200-360
	Medium amount	600-2000	36-60	360-600

Case 1: Data stealing: The malware updates the login form to delude the target into submitting a one time password combined with the login details. This info is employed by the scammer to execute a trade (with a high value) against a personal account, where the recipient hadn't sent money to. We assess both the situation of the communication coming from a national and foreign IP location. To introduce the fraud, we sporadically picked a victim from the investigating dataset and used an unplanned timestamp for the trade.

Case 2: Abducting a payment process: Via spoofing the victim's web browser. The Trojan—not the scammer—takes charge of a real bank transfer. This link is made achievable by the victim's device and IP address, which raises a problem. To mimic a session spoofing, we additionally carry out a fraudulent transaction ten minutes shortly after the true one.

Case 3: Covert Deception: The goal of the counterfeiters is to implement a series of low–medium size transactions, renewed regularly for one month during working hours, to perfectly merge in. We assess three occasions (extremely low, low and medium daily doses). We recreate the total amount of users from the preceding cases, with every single one conducting thirty forged transactions.

Hybrid Cases: Abducting a payment process and Data stealing:

In order to give a more plausible analyze and empirical evidence for the sustainability of our methodology, we assess BankSealer in connection with the frauds equally established from the first two cases, in addition to investigating each scenario separately.

4.4 Measurements and estimation style

We employed the identical assessment standards that were previously laid out. We introduce m forged transactions into the evaluation dataset subsequent training. Then, centered on the relevant anomaly assessments, we grade persons and money transfers using the time-based profiles and regional profiles, correspondingly. The intent of the universal profiles is to decrease inadequate training. Where m is the total amount of infused transactions (or users), we check out the top m activities (or users) in the leaderboard. In this scenario, m indicates 1% of the information set utilized to conduct testing. According to the specific situations, an illicit activity might toggle off the time-based profile, the nearby profile, or both. The quantity of forged payments (or users) in the top m spots are included as authentic positives, meanwhile the balance of transactions (to the total m) are seen as false positives. To eliminate biases, every experiment is run ten times, and the outcomes are averaged.

The entire outcome are in harmony with what was achieved, illustrated in Figure 4.2 and Figure 4.3, with BankSealer outperforming the existing state of the knowledge. For instance, this approach catches up to 60–70% of fraudsters with unidentified accuracy. Surprisingly inadequate training has a small portion of an impact.

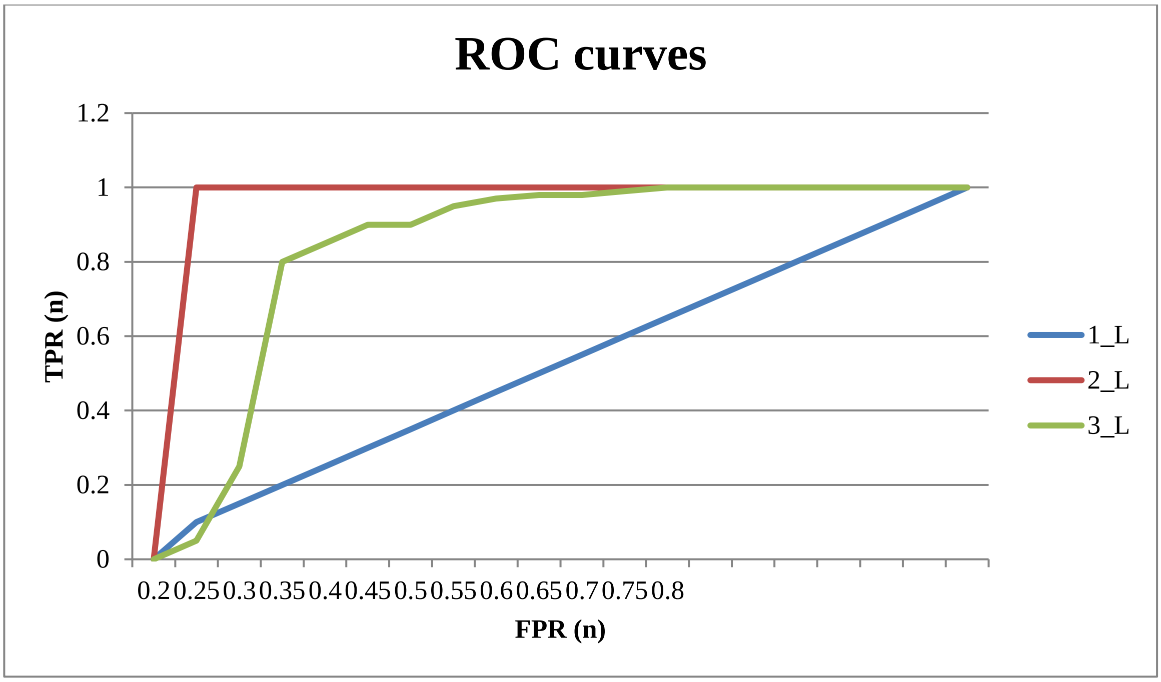

Fig. 4.2. True Positive Rate (TPR) and False Positive Rate (FPR) for $m \in [1, M]$

Here, in this equationm $\in [1, \mathrm{M}]$, M is the size of where N is the sample dataset's quantity. "UT" symbolizes "under-training," "L" signifies the regional profile, and "T" signifies the time-based profile. BankSealer functions identically in Scenarios 1, 2, and mixed, demonstrating a high identification rate (about 90%) for smaller amounts of n. The third instance is most challenging and yields a 74% recognition rate because of the time-based profile.

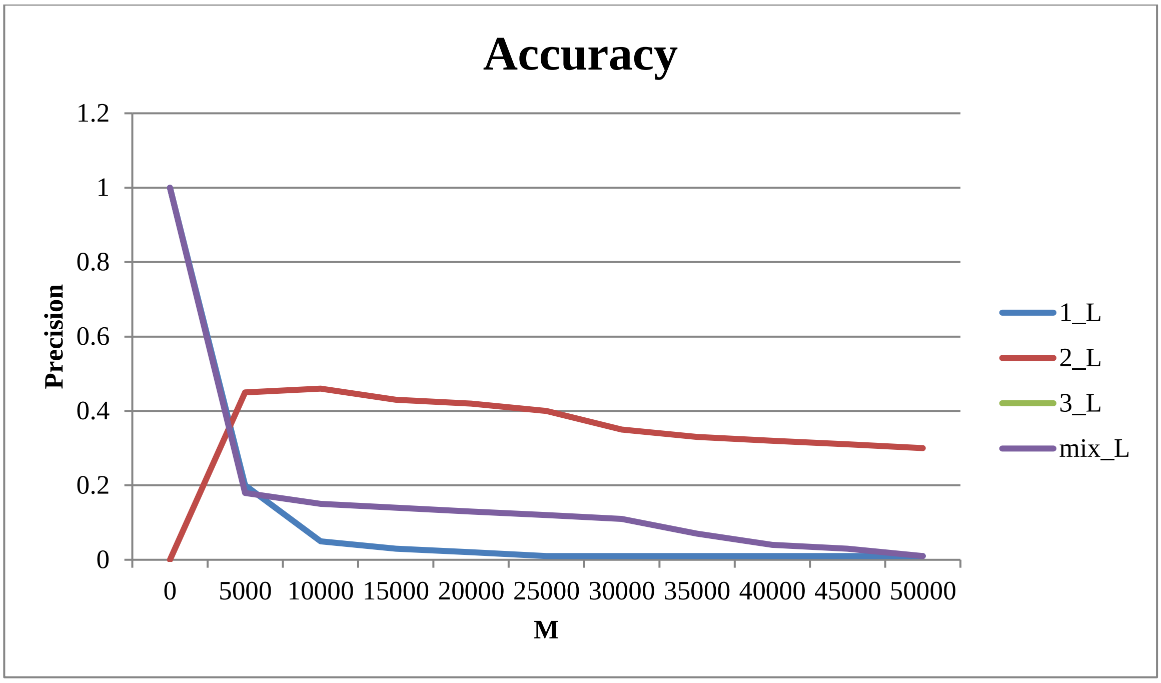

Fig. 4.3. Accuracy for $m \in [1, M]$

where M is the experimental dataset's size. "UT" refers to "under-training," "L" specifies the regional profile, and "T" signifies the temporal pattern. In Situations 1, 2, and mixed, BankSealer demonstrates good precision and a low percentage of m (around 80%). In Scenario 3, the temporal pattern boosts overall effectiveness by up to 90% in terms of precision [15].

5. Conclusion

The management of risks is always a difficult one that is not easy to refer to in multiple articles. Therefore in this research paper, the authors have proposed the DSS. These days, online fraud is extremely prevalent thus this article proposes an innovative technique called a decision support system. This DSS can help boost the financial sector and stop scams. This resulted in a determination of 49 characteristics and the associated detection of 524 threats. The Leavitt structure model's four dimensions are utilized to organize the newly established aspects. Based on the outcome of the SLR, 163 rules and 53 questions were created and these are applied in the DSS decision-making process. This DSS is downloadable on its website and is additionally employed as a tool. The DSS for identifying fraud has precisely highlighted which dubious actions have been introduced to the banking data. Additionally, the procedure has discovered extra actions that match the troubling behavior requirements alongside those that were submitted within the dataset. In so far as the technique complies with the given fashion, it is also usable with other financial databases. An individual can make adjustments to the system's output after completing further scrutiny. As long as the system complies with the supplied architecture, it may be utilized as well with different financial records. Future research subjects have been highlighted in several classifications. In a DSS venture, suggested DSS might be linked to several structuring stages. Discovering variances in DSS results at various phases of the project may be a good way to do this. On top of that, it would be fascinating to evaluate and coincide DSS's capabilities in a real-life endeavor scenario. This may be performed by calculating the expense and benefit of each danger and figuring out the right control mechanism.

References

[1] Susto, G. A., Terzi, M., Masiero, C., Pampuri, S., & Schirru, A. (2018, September). A fraud detection decision support system via human on-line behavior characterization and machine learning. In *2018 First International Conference on Artificial Intelligence for Industries (AI4I)* (pp. 9-14). IEEE.

[2] Keen, P. G. (1980, June). Decision support systems: a research perspective. In *Decision support systems: Issues and challenges: Proceedings of an international task force meeting* (pp. 23-44).

[3] Jung, D., Tran Tuan, V., Quoc Tran, D., Park, M., & Park, S. (2020). Conceptual framework of an intelligent decision support system for smart city disaster management. *Applied Sciences*, *10*(2), 666.

[4] Carminati, M., Polino, M., Continella, A., Lanzi, A., Maggi, F., & Zanero, S. (2018). Security evaluation of a banking fraud analysis system. *ACM Transactions on Privacy and Security (TOPS)*, *21*(3), 1-31.

[5] Holley, M. (2011). Decision Support Systems and Financial Risk Assessment-An evaluative study.

[6] Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not?. *Decision Support Systems*, *56*, 11-26.

[7] Naseem, A., Shah, S. T. H., Khan, S. A., & Malik, A. W. (2017). Decision support system for optimum decision making process in threat evaluation and weapon assignment: Current status, challenges and future directions. *Annual reviews in control*, *43*, 169-187.

[8] Mecati, M., Cannavò, F. E., Vetrò, A., & Torchiano, M. (2020). Identifying risks in datasets for automated decision–making. In *Electronic Government: 19th IFIP WG 8.5 International Conference, EGOV 2020, Linköping, Sweden, August 31–September 2, 2020, Proceedings 19* (pp. 332-344). Springer International Publishing.

[9] Ngai, E. W., & Wat, F. K. T. (2005). Fuzzy decision support system for risk analysis in e-commerce development. *Decision support systems*, *40*(2), 235-255.

[10] Carminati, M., Caron, R., Maggi, F., Epifani, I., & Zanero, S. (2014). BankSealer: An online banking fraud analysis and decision support system. In *ICT Systems Security and Privacy Protection: 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings 29* (pp. 380-394). Springer Berlin Heidelberg.

[11] Tyugu, E. (2011, June). Artificial intelligence in cyber defense. In *2011 3rd International conference on cyber conflict* (pp. 1-11). IEEE.

[12] Sharma, A., & Panigrahi, P. K. (2013). A review of financial accounting fraud detection based on data mining techniques. *arXiv preprint arXiv:1309.3944*.

[13] Aslam, A., Ahmad, N., Saba, T., Almazyad, A. S., Rehman, A., Anjum, A., & Khan, A. (2017). Decision support system for risk assessment and management strategies in distributed software development. *IEEE Access*, *5*, 20349-20373.

[14] Lawrencia, C., & Ce, W. (2019, August). Fraud detection decision support system for Indonesian financial institution. In *2019 International Conference on Information Management and Technology (ICIMTech)* (Vol. 1, pp. 389-394). IEEE.

[15] Carminati, M., Caron, R., Maggi, F., Epifani, I., & Zanero, S. (2015). BankSealer: A decision support system for online banking fraud analysis and investigation. *computers & security*, *53*, 175-186.