ISSN: 2182-2069 / E-ISSN: 2182-2077

Optimized Spammer Detection System for Enhancing Financial Cloud Security Through Artificial intelligence

Chethan Venkatesh[1*], Vinay Kumar Sadolalu Boregowda[2], Sukhman Ghumman[3], Debanjan Ghosh[4], Shoaib Mohammed[5], and Deepali Rani Sahoo[6]

[1*]Associate Professor, Department of MCA, RV Institute of Technology and Management, Bangalore, Affiliated to VTU, India. chethu4u@gmail.com, https://orcid.org/0000-0001-8009-6409

[2]Assistant Professor, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Bangalore, Karnataka, India. sb.vinaykumar@jainuniversity.ac.in, https://orcid.org/0000-0001-7349-1697

[3]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. sukhman.ghumman.orp@chitkara.edu.in, https://orcid.org/0009-0005-2008-1009

[4]Assistant Professor, Department of Computer Science & IT, ARKA JAIN University, Jamshedpur, Jharkhand, India. debanjan.g@arkajainuniversity.ac.in, https://orcid.org/0000-0002-3255-6199

[5]Assistant Professor, Department of ISME, ATLAS SkillTech University, Mumbai, Maharashtra, India. shoaib.mohammed@atlasuniversity.edu.in, https://orcid.org/0009-0003-7819-1484

[6]Associate Professor, Manipal Law School, Jaipur, Manipal University, India. sahoodeepali4u@gmail.com, https://orcid.org/0000-0001-6949-7439

Received: February 04, 2025; Revised: March 18, 2025; Accepted: April 28, 2025; Published: May 30, 2025

Abstract

Financial cloud services have many improvements, but there are also deliberate security dangers, one of which is spamming. Furthermore, changing the spamming approach may have an impact on the model's efficiency and necessitate growing upgrades and developments. In this research, we introduce a unique technique, Dynamic Transient Search-driven Random Forest (DTS-RF), to advance and execute a capable Spam Detection System (SDS) that leverages to augment the security of financial transactions within cloud platforms. Research collected the dataset as an extensive collection of both legitimate and spam-related activity. A crucial step in getting the dataset prepared for SDS training is data cleansing. It requires eliminating noise, inconsistencies and extraneous information from the data to ensure model predictions are specific and dependable. The most pertinent and instructive characteristics are identified for the SDS's training by applying Independent Component Analysis (ICA) to feature extraction. Based on the suggested methodology, this study is carried out using the Python program and performance is examined in terms of accuracy (94%), precision (95.7%), recall (92.7%) and F1-score (93.5%). The solution achieves strong performance

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 362-373.
DOI: *10.58346/JISIS.2025.I2.026*

*Corresponding author: Associate Professor, Department of MCA, RV Institute of Technology and Management, Bangalore, Affiliated to VTU, India.

and increases the total resilience of financial networks towards spamming threats by combining DTS-RF.

Keywords: Dynamic Transient Search-driven Random Forest (DTS-RF), Spammer Detection System (SDS), Financial Cloud Security.

1 Introduction

The Internet of Things (IoT) holds significant importance as a fundamental element within the framework of contemporary information and Financial Cloud Security systems. Darapour, (2016). Intelligent awareness, recognition technology and distributed computing are employed in several domains, including corporate control, networked physical systems and combat intelligence (Feng et al., 2018). The fundamental concept of IoT is to comprehend and quantify the environment by examining the interconnections among things in the vicinity of individuals Alnumay, (2024). This concept relies on the Internet and interfaces to facilitate interaction among devices. The utilization of enabling technology facilitates the connection between humans and things and materials with objects, hence permitting remote control and the management of intelligent networks in innovative approaches (Osa & VO, 2021).

Encompassing both human-object control and human-machine control is a crucial aspect of the IoT. It serves as a fundamental basis for attaining intelligence (Ojugo et al., 2023). This holds significant importance in the context of contemporary manufacturing. Spammers target the mobile network because of its significance in manufacturing control (Sokolov et al., 2019). Spam is a prevalent type of attack within mobile networks. The purpose is to identify spammers who impersonate regular users and exclusively send unwanted messages. An issue of significant concern arising from spam is the inadvertent selection of links that lead to viruses, resulting in the theft of users' data or interference with operational management (Afzal et al., 2021). The malignant nodes engage in communication with one another, while spammers conceal themselves among them, as depicted in Figure 1. The left-hand side of the net structure depicts character visuals that indicate mobile cloud computing and financial cloud security, while the right-hand side describes the behaviour data of each user (Reddy & Thomas, 2024). In the environment, the red character images are indicative of spammers, whereas the green ones symbolize regular users (Shrmali & Sharma, 2022).

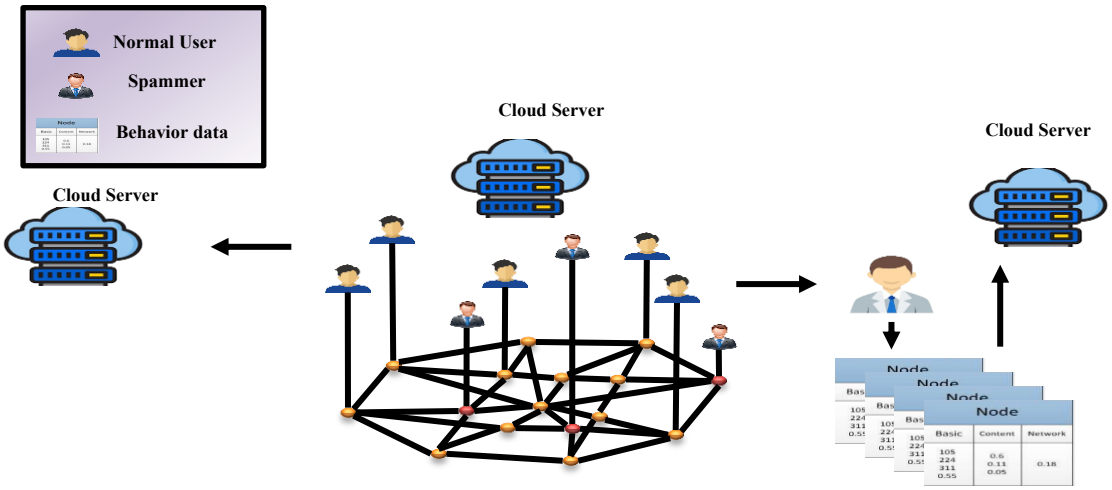

Figure 1: Spammers in Financial Cloud Security (Source: author)

The essential purpose of financial cloud security for SDS is to employ exceptional methods, along with machine learning methods, pattern recognition and behavioural analytics, to adeptly recognize and anticipate spam attacks. The SDS can dynamically detect and mitigate potential risks before they expand by constantly monitoring network traffic, analyzing user behaviours and recognizing suspicious trends (Gomathi et al., 2020). Moreover, the technology provides transitory alerts and notifications, enabling security experts to instantly respond to potential individuals as well as to prevent unauthorized entry or data breaches. The system's intelligence to adapt allows it to develop and modify to innovative spamming methods and maintain an aggressive defence plan toward ever-changing cyber threats (Rabbani et al., 2020). In this research, an innovative technique, DTS-RF, to enhance and performance accomplished DS that leveraged to augment the security of financial transactions within cloud platforms.

There is a list of related works in Section 2. In section 3, the methodology is presented. Section 4 is indicated in the findings. The conclusion is presented in section 5.

2 Related Works

Fathin et al., (2023) proposed a machine learning (ML) technique designed to recognize fraudulent identities within social media networks. The system provided actual identification of spammers without conditional on unpredictable and inconsistent communication. Siti & Putri, (2025). The Spammer Identification schemes depend on the Gaussian Mixture Model (SIGMM)structure incorporates the integration of data visualization with the model development process, wherein a class was specified to every user node.

Gadde et al., (2021) employed a range of ML and deep learning (DL) methodologies to detect Short Message Service (SMS) spam. The experimental findings showed that the Long Short-Term Memory (LSTM) model demonstrated effective performance compared to preceding models in the field of spam identification, with an accuracy rate of 98.5%.

Khan et al., (2022) presented that an ML model was employed the provided structure to detect spam characteristics of IoT devices. The utilization of ML techniques in the environment can enhance the convenience and security of IoT systems by employing anomaly detection as well as establishing security and authorization through biometrics.

Sun et al., (2022) introduced a system whose purpose is to detect spam on Twitter in near real-time. The method involved acquiring tweet data in near real-time, extracting lightweight characteristics from a “single Twitter account”, training a recognition method and explicitly representing the detection observations online. The model's ability to attain good efficiency based on the information had been confirmed by empirical findings.

Ning et al., (2025) investigated the influence of digital transformation on the probability of market price crashes in publicly traded businesses. The research utilized a 2-way fixed influence concept that incorporated both duration and particular variables. Simultaneously, it enhanced theoretical investigation into the influence of the digital revolution on microeconomic units and offered possible insights along with proof for firms to expedite the online transition (Arasuraja, 2024).

Nguyen et al., (2018) employed a DL methodology to identify cyberattacks in a mobile cloud setting. The experimental findings provided evidence that the suggested learning model exhibited a notable level of accuracy in the detection of cyberattacks, surpassing alternative ML approaches (Kapoor & Malhotra, 2025).

Sangaiah et al., (2019) proposed a methodology for preserving the secrecy of the situation for users of roaming "Position-based services (PBSs)" through the utilization of ML methods. Extensive experimental investigations were undertaken, thereby confirming that the proposed methodology successfully attained a position confidentiality rate exceeding 90% in PBSs.

3 Methodology

3.1 Data Collection

The Enron database was selected for the investigation due to its status as a unique, comprehensive collection of publicly available emails and its widespread utilization among experts. The Enron database has six primary directories, with each directory comprising several subdivisions, each holding individual text files holding emails. The above-mentioned emails were consolidated into a unified Comma-Separated Values (CSV) file. Approximately 33,000 emails were present in the CSV file. Nevertheless, during the process of conversion, certain email messages exhibited a lack of accurate alignment with their respective labels. The messages that did not align were eliminated, together with the orphaned labels, using Microsoft Excel. After the elimination process was finished, of the entire emails, 16,834, 51 per cent were spam 16,026 49 per cent were legitimate (ham). The CSV file held a overall of 32,860 emails. In the CSV file, there were five distinct columns denoted asspam/ham, communication identification, topic and date (Omotehinwa & Oyewola, 2023).

3.2 Data Cleaning

Data cleaning is the systematic procedure of identifying and rectifying or eliminating erroneous, deficient, or irrelevant components of data. The method of data analysis and processing is of utmost importance as it guarantees the accuracy, consistency and reliability of the data utilized for analysis. Data duplication can be identified by doing a comparison of rows or columns and eliminating or combining elements that are identical or substantially similar. This practice guarantees the uniqueness of every data point and minimizes redundancy within the information.

3.3 Feature Extraction by Using Independent Component Analysis (ICA)

ICA is a recently developed statistical and computational methodology that is employed to uncover latent components within a dataset of measurements or observed data, with the intention of achieving maximum independence among the sources.

Mathematically, the function $w(s) = w_1(s), w_2(s), \ldots\ldots, w_m(s)$can be written as a linear combination of the originating and conditionally independent inputs at a given time point, assuming the measured elements $t(s) = t_1(s), t_2(s), \ldots\ldots, t_m(s)$ As shown in equation (1).

$$w(s) = As(s) \tag{1}$$

The vector A Represents a full-rank mixture vector. In the context of ICA standards, Equation (1) is commonly expressed as in Equation (2):

$$z = Xw \tag{2}$$

The de-mixing vector, denoted as $X = B^{-1}$, is used to represent the independent element, denoted as $z = z_1, z_2, \ldots., z_m$. The purpose is to determine the demixing vector and independent elements

exclusively using the combined information. This can be achieved using different ICA algorithms such as fastICA, Joint Approximate Diagonalisation of Eigenmatrices (JADE), Info-max and others.

In the ICA estimate, the recovered elements are characterized by their non-Gaussian nature and independence. Kurtosis denoted asβ_1, is a statistical measure used to assess non-Gaussianity. The kurtosis value of the Gaussian ICs is 0; for sub-Gaussian ICs, it is$\beta_1 \leq 0$, and for super-Gaussian ICs it is$\beta_1 \geq 0$. The conventional metric for kurtosis is formally defined as in equation (3).

$$\beta_1 = \frac{F(w-\mu)^4}{(E(w-\mu)^2)^2} - 3 = \frac{\mu_4}{\sigma^4} - 3 \tag{3}$$

The standard metrics of kurtosis, which rely on sample averages, are susceptible to the influence of outliers. Furthermore, the influence of outliers is magnified in the traditional kurtosis metrics since they are exponentiated to the third and fourth powers. To address the aforementioned issue, research endeavours to employ a robust measure of kurtosis in the setting of ICA as shown in equation (4).

$$Kurtosis = \frac{(F_7-F_5)+(F_3-F_1)}{(F_6-F_2)} \tag{4}$$

A proposed substitute for the quantity of Moors' kurtosis is the quantile kurtosis, denoted asF_j where $F_j$represents the j^{th}octile. This can be expressed as$F_j = E^{-1}\left(\frac{j}{8}\right)$. The quantile kurtosis for Gaussian independent elements is 1.23. One notable benefit of utilizing quantile metrics for kurtosis is their independence from the first and second moments. The robustness of this measure surpasses that of the standard measure of kurtosis. ICA is a valuable dimension, maintaining modification in pattern categorization as it generates mathematically independent elements.

3.4 Dynamic Transient Search-driven Random Forest (DTS-RF)

To identify spammer activity in real-time, it entails using a DTS-RF to find temporary patterns in data. Through the incorporation of this technique into RF architecture, the system can detect and mitigate spamming risks in financial cloud settings with greater effectiveness and performance, hence strengthening overall security mechanisms.

3.4.1 DTS Optimization

The opposing learning strategy (OLS) is used in the effort to optimize the exploration and exploitation of the dynamic Transient Search Optimisation algorithm (DTSOA) and increase the converging performance. Due to the optimization variable being chosen arbitrarily and the techniques' lack of ideal domain search and critical criterion information, these techniques may become caught in local optimal performance. Additionally, because of the discrepancy between the initial and ideal responses, these techniques take a lot of time. These techniques might not have adequate converging velocity and correctness, even if they manage to achieve the global optimal. To find a substitute for the current solution, DTSOA employs OLS. This method makes it possible to approach and arrive at the ideal solution. As a result, the rate of convergence quickens. Let W be in $[\eta, \lambda]$ the other point $\overline{W} = \eta + \lambda - W$. A point in the search space with dimension c is denoted by$W = (W_1, W_2, \cdots, X_c)$; here, $W_1, W_2, \cdots, W_c \epsilon Q$and $W_j \epsilon \left[\eta_j, \lambda_j\right], \forall j \in \{1,2, \cdots \cdots, c\}$ according to its constituents, the opposing point is as below in equation (5).

$$\overline{W} = \eta_j + \lambda_j - W_j, \overline{W} = (\overline{W_1}, \overline{W_2}, \cdots \cdots, \overline{W_c}) \tag{5}$$

Thus, the OLS is used to construct the initial sample.

Additionally, a nonlinearly decreasing strategy (NDS) is used to attain a desired balance among global converging and divergent effectiveness and enhance the DTSOA performance in both local and global exploring. The optimization of search efficiency can be achieved by adjusting the ∂^{NSD}Coefficient. From $\partial_{max}^{NDS}$to∂_{min}^{NDS}, the ∂^{NSD}decreased nonlinearlya higher significance value for ∂^{NSD} contributes to improved global search capacity. Additionally, during the exploration phase, the lower ∂^{NSD}improves global search capabilities. This tactic is inspired by equation (6).

$$\partial^{NSD} = \partial_{max}^{NDS} - \frac{JS \times (\partial_{max}^{NDS} - \partial_{min}^{NDS})}{JS^{max}} \times \sin\left(\frac{JS \times \pi}{2 \times JS^{max}}\right) \quad (6)$$

Where the terms $\partial_{max}^{NDS}$and ∂_{min}^{NDS} denote the coefficient's maximum and minimum bounds, correspondingly in equation (7).

$$\begin{cases} \partial^{NSD} W_{JS}^{*ab} + \left(W_{JS} - VW_{JS}^{*ab}\right) f^{-\alpha}; qn_l < 0.5 \\ \partial^{NSD} W_{JS}^{*ab} + \left|W_{JS} - VW_{JS}^{*ab}\right| f^{-\alpha} \ (\cos(2\pi\alpha) + \sin(2\pi\alpha)); \quad qn_l < 0.5 \end{cases} \quad (7)$$

Lastly, the DTSOA's converging rate is quick and it can do a high-capacity global search during pre-search.

3.4.2 RF Algorithm

Based on the decision tree (DT) concept, the RF algorithm is an aggregate classification algorithm. Employing bootstrap collection, it creates$l$distinct subsets of training data from identical information. These categories are trained to create lDT. Finally, these DT are combined to create an RF. Every DT predicts a sample from the testing dataset and the results from these trees determine the overall classification outcome that is provided.

$T = \{(w_j, z_i)\}, j = 1,2,\cdots, M; i = 1,2,\cdots N\}$ is the formal representation of the first training dataset, in which w represents a sample z and Tits a feature variable. Specifically, each of the Msamples in the distinctive training dataset have Nfeature variables.

The following are the stages involved in creating the RF algorithm.

- **Sampling$l$training Subsets**

Using the bootstrap collection, l training subsets are selected in this stage from the initial training dataset$T$. Specifically, a random sampling and replacement mechanism is used to select Mrecords from T At each sample period. Following the present phase, several training subsets $T_{Train}$is used to create l training subsets as shown in equation (8).

$$T_{Train} = \{T_1, T_2, \cdots T_l\} \quad (8)$$

Simultaneously, each sample period's non-selectable records are combined into an Out-Of-Bag (OOB) collection. This is how a collection of $T_{ooB}$is built into l OOB sets. A shown in equation (9).

$$T_{ooA} = \{OOA_1, OOA_2, \cdots, OOA_l) \quad (9)$$

Where$T_j \cap OOB_j = T$,$T_j \cap OOB_j = \emptyset$and$l \ll M$,following the training phase, these OOB sets are utilized as testing sets to determine every tree model's categorization efficiency.

- **Constructing Each DT Model**

A C4.5 or CART algorithm creates every MetaDT in an RF model from every training sampleT_j. During the tree-growth procedure, $n$feature variables from datasetT_j are chosen at random from a list of Nvariables. The best feature variable is selected as the splitting node in every tree node splitting manipulation, which involves calculating the gain ratio of every feature variable. Until a leaf node is produced, this splitting procedure is continued. Lastly, the same training procedure is used to train lDTs from $l$training subsets.

- **Collecting $l$trees into an RF Model**

Equation (10) defines an RF model, which is comprised of the l trained trees as shown in equation (10).

$$G = (W, \Theta\, i)(i = 1,2, \cdots \cdots, n) \tag{10}$$

Where $W$the input characteristic matrices of the training dataset is, $\Theta i$is an autonomous, identically distributed random matrix that controls the tree's growth procedure and $g_j(w, \Theta i)$is a MetaDT classifier.

4 Results

Research implemented our approach in Python (v 1.8), and the system configuration includes Pytorch1.14, compatible with Python 1.8, on a Windows 11 OS. The suggested technique is examined in regard to precision (%), accuracy (%), F1-score (%), and recall (%) compared with the existing approaches, which are "Random forest (RF), Decision tree (DT), Hybrid bagging (HB)" (Rayan, 2022).

Accuracy metrics assess the efficacy of the system in detecting spammers and improving financial cloud security. A comparison of accuracy is presented in Figure 2. Our suggested DTS-RF approach performed (94%), in contrast to (84%), (92%), and (88%) of the current techniques such as RF, DT and HB. The outcomes demonstrate that the suggested strategy outperforms existing methods.

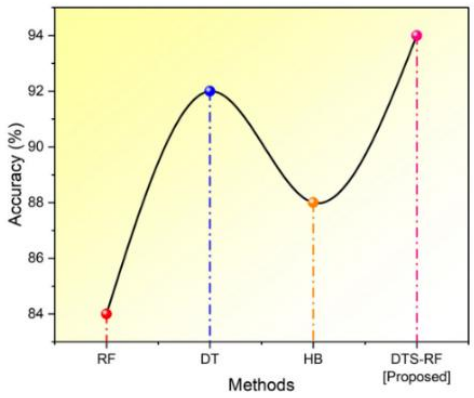

Figure 2: Result of Accuracy (Source: author)

Precision metric quantifies the ratio of identified spammers to the total number of flagged cases, hence facilitating the evaluation of financial cloud system efficiency. A precision comparison is shown in Figure 3. While the existing methods, RF, DT, and HB, achieved (85%), (94%), and (90%), respectively, our proposed DTS-RF methodology achieved (95.7%). The findings demonstrate that our suggested approach outperforms existing methods substantially.

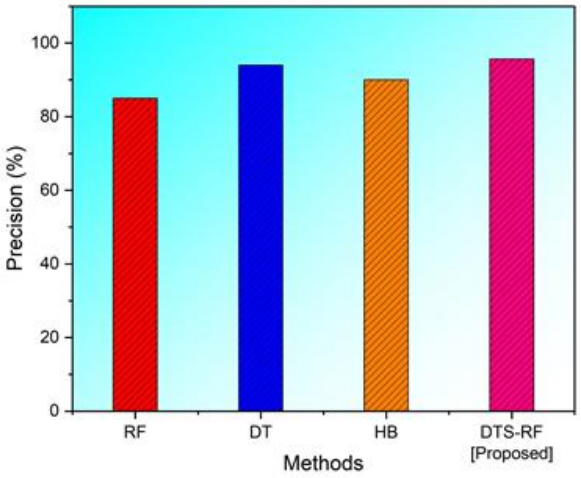

Figure 3: Result of Precision (Source: author)

A recall metric is utilized to assess the system's capacity to accurately detect spam in financial cloud security comparison to instances where spam is disregarded. Figure 4 provides a comparative analysis of recall. The DTS-RF strategy research proposes and achieves a recall of (92.7%), which is superior to the memory of the existing techniques RF (82%), DT (90%) and HB (86%). The outcomes demonstrate that our proposed approach outperforms the current methods by a substantial margin in terms of recall.

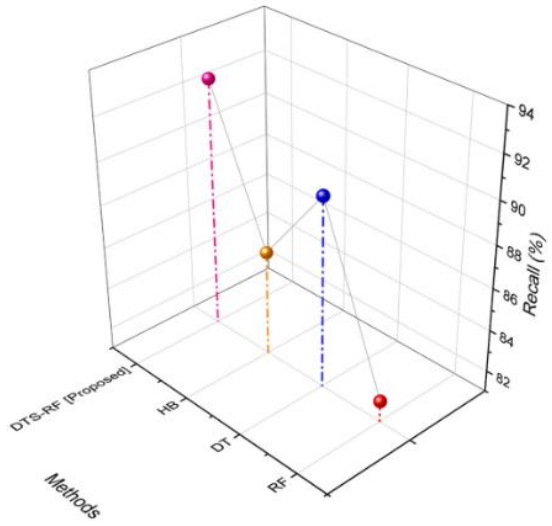

Figure 4: Result of Recall (Source: author)

F1-score metrics assess the system's ability to reliably identify spammers and the number of spammers it correctly observes, which is essential for improving financial cloud security. Figure 5 displays a comparative assessment of the F1-score. The DTS-RF method propose and achieved an F1-score of (93.5%), which is better than the memory of the traditional methods RF (90%), DT (85%), and HB (88%). The findings shows that our suggested method surpasses the traditional methods by a generous margin regarding the F1-score. Table 1 shows the overall result comparison.

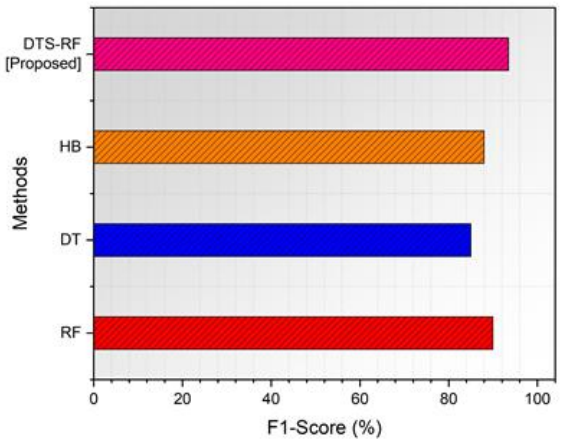

Figure 5: Result of F1-score (Source: author)

Table 1: Overall Result Comparison (Source: author)

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
RF	84%	85%	82%	90%
DT	92%	94%	90%	85%
HB	88%	90%	86%	88%
DTS-RF [Proposed method]	94%	95.7%	92.7%	93.5%

5 Conclusion

The study proposed a unique approach, DTS-RF for effective the security of financial cloud services by combating spamming hazards. To perform effective model forecasting, this investigation emphasizes the significance of a substantial database, data cleansing to ensure the quality and authenticity of the dataset and feature extraction employing ICA. Through authentic valuation using Python programming, the proposed solution indicated strong performance metrics including accuracy (94%), precision (95.7%), recall (92.7%), and F1-score (93.5%). These findings indicate the DTS-RF standard works to strengthen financial network defences against spamming techniques. This technique highlights the essential of continuous updates and developments in enduring strong security protocols inside financial cloud services. It also maximized the conventional flexibility of financial networks towards developing spamming methods. All of these benefits come at the consumption of increased model performance. The reliance on DTS-RF for Spammer Detection in Financial Cloud Security on up-to-date data could cause a suspension in restoring to new spamming approaches. Future plans comprise aggregate overall security measures with enhanced real-time flexibility, improved AI approaches and block-chain technology for immutable data verification.

References

[1] Afzal, S., Asim, M., Javed, A. R., Beg, M. O., & Baker, T. (2021). Urldeepdetect: A deep learning approach for detecting malicious urls using semantic vector models. *Journal of Network and Systems Management*, *29*(3), 21. https://doi.org/10.1007/s10922-021-09587-8

[2] Alnumay, W. S. (2024). The past and future trends in IoT research. *National Journal of Antennas and Propagation, 6*(1), 13–22.

[3] Arasuraja, G. (2024). Organizational Change Management in Digital Transformation: A Framework for Success. *Global Perspectives in Management*, *2*(2), 12-21.

[4] Darapour, M. (2016). The role of toxic assets in the formation of financial crisis (Case study: Iran central bank's monetary system). *International Academic Journal of Organizational Behavior and Human Resource Management, 3*(2), 1–7.

[5] Fathin, F. A., Rizwana, A., & Afrah, J. (2023). Spammer Identification Using Novel Machine Learning Algorithm in Industrial Mobile Cloud Computing. *International Journal of Research in Engineering, Science and Management, 6*(9), 38-42.

[6] Feng, B., Fu, Q., Dong, M., Guo, D., & Li, Q. (2018). Multistage and elastic spam detection in mobile social networks through deep learning. *IEEE Network*, *32*(4), 15-21. https://doi.org/10.1109/MNET.2018.1700406

[7] Gadde, S., Lakshmanarao, A., & Satyanarayana, S. (2021, March). SMS spam detection using machine learning and deep learning techniques. In *2021 7th international conference on advanced computing and communication systems (ICACCS)* (Vol. 1, pp. 358-362). IEEE. https://doi.org/10.1109/ICACCS51430.2021.9441783

[8] Gomathi, S., Parmar, N., Devi, J., & Patel, N. (2020, September). Detecting malware attack on cloud using deep learning vector quantization. In *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 356-361). IEEE. https://doi.org/10.1109/CICN49253.2020.9242574

[9] Kapoor, P., & Malhotra, R. (2025). Zero Trust Architecture for Enhanced Cybersecurity. In *Essentials in Cyber Defence* (pp. 56-73). Periodic Series in Multidisciplinary Studies

[10] Khan, A. A., Mulajkar, R. M., Khan, V. N., Sonkar, S. K., & Takale, D. G. (2022). A research on efficient spam detection technique for IoT devices using machine learning. *Neuro Quantology*, *20*(18), 625-631.

[11] Nguyen, K. K., Hoang, D. T., Niyato, D., Wang, P., Nguyen, D., & Dutkiewicz, E. (2018, April). Cyberattack detection in mobile cloud computing: A deep learning approach. In *2018 IEEE wireless communications and networking conference (WCNC)* (pp. 1-6). IEEE. https://doi.org/10.1109/WCNC.2018.8376973

[12] Ning, F., Jin, J., Zhang, L., & Wang, D. (2025). Risk analysis of China's financial market collapse based on cloud computing and machine learning algorithms. *Expert Systems*, *42*(1), e13426. https://doi.org/10.1111/exsy.13426

[13] Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Odiakaose, C., & Emordi, F. U. (2023). DeGATraMoNN: Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing. *Kongzhi yu Juece/Control Decis*, *38*(01), 667-678.

[14] Omotehinwa, T. O., & Oyewola, D. O. (2023). Hyperparameter optimization of ensemble models for spam email detection. *Applied Sciences*, *13*(3), 1971. https://doi.org/10.3390/app13031971

[15] Osa, E., & VO, E. (2021). Modelling of a Deep Learning Based SMS Spam Detection Application. *NIPES-Journal of Science and Technology Research*, *3*(4).

[16] Rabbani, M., Wang, Y. L., Khoshkangini, R., Jelodar, H., Zhao, R., & Hu, P. (2020). A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing. *Journal of Network and Computer Applications*, *151*, 102507. https://doi.org/10.1016/j.jnca.2019.102507

[17] Rayan, A. (2022). Analysis of e-Mail Spam Detection Using a Novel Machine Learning-Based Hybrid Bagging Technique. *Computational Intelligence and Neuroscience*, *2022*(1), 2500772. https://doi.org/10.1155/2022/2500772

[18] Reddy, S., & Thomas, E. (2024). Green Finance Mechanisms and their Impact on Sustainable SME Development. *International Journal of SDG's Prospects and Breakthroughs, 2*(2), 14-16.

[19] Sangaiah, A. K., Medhane, D. V., Han, T., Hossain, M. S., & Muhammad, G. (2019). Enforcing position-based confidentiality with machine learning paradigm through mobile edge computing in real-time industrial informatics. *IEEE Transactions on Industrial Informatics*, *15*(7), 4189-4196. https://doi.org/10.1109/TII.2019.2898174

[20] Shrmali, D., & Sharma, S. (2022). Applications of Deep Learning in Cloud Security. *Deep Learning Approaches to Cloud Security*, 225-256. https://doi.org/10.1002/9781119760542.ch14

[21] Siti, A., & Putri, B. (2025). Enhancing performance of IoT sensor network on machine learning algorithms. *Journal of Wireless Sensor Networks and IoT, 2*(1), 13-19.

[22] Sokolov, S. A., Iliev, T. B., & Stoyanov, I. S. (2019, May). Analysis of cybersecurity threats in cloud applications using deep learning techniques. In *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 441-446). IEEE. https://doi.org/10.23919/MIPRO.2019.8756755

[23] Sun, N., Lin, G., Qiu, J., & Rimba, P. (2022). Near real-time twitter spam detection with machine learning techniques. *International Journal of Computers and Applications*, *44*(4), 338-348. https://doi.org/10.1080/1206212X.2020.1751387

Authors Biography

Dr. Chethan Venkatesh joined RV Institute of Technology and Management (RVITM), Bengaluru in 2023. He is serving as Associate Professor in the Department of Master of Computer Applications. He received his Ph.D. in Computer and Information Sciences from the Computer Science and Engineering Department, Visvesvaraya Technological University (VTU), Belagavi in 2023, M.Phil in Computer Science from Bharathidasan University, Thruchirappali, MCA from Dr. AIT, Bengaluru. He has 21 years of Teaching and 10 years of Research experience. Prior to RVITM he has worked in MSRIT (2006-2023), SirMVIT (2004- 2006), and AMCEC (2002-2004). He is a member of IEEE, life member of ISTE, CSI and IAENG.

S.B. Vinay Kumar is an Assistant Professor in the Department of Electronics and Communication Engineering at the School of Engineering and Technology, Jain (Deemed-to-be University), Bangalore. He holds an M.Tech in Signal Processing and VLSI and is currently pursuing a Ph.D. in ECE. His research interests include VLSI, reverse logic, DSP, and embedded systems. He has published 13 papers in international journals indexed in Scopus and others, and has presented at multiple national and international conferences. He has also completed three sponsored research projects funded by KSCST and IISc Bangalore.

Sukhman Ghumman is affiliated with the Centre of Research Impact and Outcome at Chitkara University, Rajpura, Punjab, India. She is engaged in interdisciplinary research contributing to innovation and academic excellence at the institution. Her research interests span across emerging domains in science and technology. She actively contributes to collaborative projects aimed at societal impact and scholarly development.

Debanjan Ghosh is an Assistant Professor in the Department of Computer Science & IT at ARKA JAIN University, Jamshedpur, Jharkhand, India. He specializes in computer science education and research with a focus on emerging IT technologies. Debanjan actively contributes to academic research and curriculum development. His work supports advancements in information technology and computing applications.

Dr. Shoaib Mohammed is an Assistant Professor in the Department of ISME at ATLAS SkillTech University, Mumbai, Maharashtra, India. He specializes in interdisciplinary management and social sciences, contributing to research and academic excellence. Dr. Mohammed is actively involved in advancing knowledge through teaching, research, and community engagement.

Dr. Deepali Rani Sahoo, working as an Associate Professor in the Department of Law, Manipal University, Jaipur. I have 13 years of teaching and research experiences in other private Universities as well. In regards to research and publications, I have a total of approximately 95 research articles published in various UGC Care Listed, Peer reviewed Journals (National and International) and SCOPUS Journals (10 articles published and indexed) and (4 articles published, waiting to be indexed) 7 articles are in process. I have attended and participated in various FDPs (National and International) and completed 2 MOOC courses. I have been awarded for various positions at the National and International level for teaching, learning and research.