



International Journal of Marketing Management

ISSN 2454 - 5007



www.ijmm.net

Email ID: editor@ijmm.net , ijmm.editor9@gmail.com

TRANSFORMING CUSTOMER EXPERIENCE IN BANKING WITH CLOUD-BASED ROBO-ADVISORS AND CHATBOT INTEGRATION

¹Rajeswaran Ayyadurai

Login Services
Coimbatore, India

rajeswaranayyadurai@arbpo.com

²Vinayagam.S

VRS college of engineering and technology,
Villupuram India

vinayagamss9976@gmail.com

Abstract

In this paper, the integration of cloud-based technology in banking services has been discussed in the form of the creation of AI-driven chatbots, robo-advisors, and data encryption methods for enhancing customer experience and security. The paper initially presents the Bank Transaction Data dataset that has been utilized for fraud detection and money laundering prevention based on transaction categorization and pattern identification. A prototype for cloud-based chatbot integration is then presented, one that would automate customer inquiries and enhance user experience through the use of AWS services like Amazon Lex, Lambda, and Cognito. The paper also discusses AI-powered robo-advisors that use past history and market trends and offer customized financial advice. Deep Belief Network (DBN) is used for financial decision-making in order to boost predictive correctness with 94.2% versus conventional methods. In addition, the DBN model also speeds up transaction levels by 37% when compared to SCF conventional procedures and decreases the percentage of fraud transactions by 82%, while the financial level is increased, so it improves security. Some techniques like AES-256 for encrypted data storing and privacy protection, and also the Role-Based Access Control (RBAC), assure authorized access of users. Lastly, the performance of such cloud solutions is measured through measures of performance such as response time, recommendation quality, and customer satisfaction.

Keywords: Cloud Computing, AI-powered Chatbot, Robo-Advisors, Deep Belief Network, Fraud Detection, Money Laundering, AES-256 Encryption, Role-Based Access Control Data Encryption.

1 Introduction

Cloud computing has already revolutionized many industries, such as banking, by automating customer experience, AI-based interactions, and frictionless digital banking services. It offers quality, low-cost internet-based solutions that improve customer engagement and business efficiency [1]. This is a revolutionary change in the banking sector where more banks are using cloud-based robo-advisors and chatbot integration to achieve maximum customer satisfaction and service optimization. The categorization of major concepts and methodologies is the initial step in any exhaustive study [2]. From the examination of recent developments in cloud computing, several methods have arisen, providing functional descriptions for its application in banking [3]. Cloud computing decouples application and customer data resources from the supporting infrastructure, allowing for unobstructed service delivery. It allows banks to provide AI-driven robo-advisors to help customers with customized financial planning with integrated chatbots for live support and transactional aid. Cloud computing in the banking space goes way beyond mere automation [4]. It covers a variety of functions, ranging from AI-based financial advisory services, loan processing through automation, and live fraud detection. Public cloud platforms enable financial institutions to scale services effectively, and private cloud systems provide data protection and regulatory requirements [5]. The integration of software-as-a-service models and AI-based banking solutions increases the personalization of services, increasing accessibility and efficiency in banking.

Cloud banking services provide scalability, quick responsiveness, and economical solutions to banks. Nevertheless, even with these benefits, security issues are a key challenge [6]. The cloud-based robo-advisors and chatbot platforms need strong security features, such as encryption, identity authentication, and fraud protection

mechanisms, to maintain customer confidence and data confidentiality. While cloud-based chatbot integration enhances response time and effectiveness, AI-powered robo-advisors maximize financial advice by processing enormous amounts of customer data [7]. Such services, when implemented properly, enhance customer interaction, increase operational effectiveness, and give banks a competitive advantage in the digital age. Major financial institutions are constantly assessing the security and privacy features of cloud-based banking solutions [8]. Cloud computing success in the banking sector depends on proper risk management, the identification of threats, and putting security measures into place. Strong cybersecurity infrastructure coupled with AI-powered monitoring software is necessary to mitigate threats [9].

In spite of increasing significance of Supply Chain Finance (SCF) and implementation of AI-based frameworks, research mainly concentrates on classical machine learning and rule-based methods [10]. These techniques may not identify complex, non-linear patterns in finance data and have limited predictability. Furthermore, most SCF frameworks do not have a strong integration of decentralized technologies like Proof of Stake (PoS) Blockchain, which can improve security, transparency, and transaction efficiency [11]. The study fills this gap by using DBNs to enhance predictive accuracy in SCF decision-making and incorporating PoS Blockchain to provide secure and efficient transactions.

Cloud computing is revolutionizing the future of banking, with robo-advisors and chatbots becoming an integral part of customer service. The technology allows for real-time, personalized interactions, enhancing the banking experience [12]. Yet, for successful adoption, banks need to be concerned with security, compliance, and ongoing technological advancements.

1.1 Problem Statement

Conventional banking systems struggle to deliver immediate, individualized, and integrated customer experiences [13]. Prolonged wait times, ineffective support, and scarce financial advisory services trigger customer discontent. Automated financial guidance and customer support are provided by cloud-based robo-advisors and chatbots. Nevertheless, issues relating to data protection, regulatory requirements, AI precision, and integration complexity hamper implementation [14]. This essay discusses how chatbot integration and cloud-based robo-advisors can support customer experience, make banking services smoother, and effectively overcome such issues.

1.2 Objectives

- Analyze the Bank Transaction Data dataset to detect fraudulent activities such as money laundering by categorizing transactions and identifying patterns.
- Design a prototype for integrating a cloud-based chatbot within banking services to automate and streamline customer interactions, enhancing user satisfaction through AWS services.
- Evaluate the performance of AI-powered robo-advisors in providing personalized financial advice based on historical data and market trends.
- Utilize DBN to enhance predictive accuracy, risk analysis, and fraud detection for banking services.
- Use encryption methods like AES-256 and privacy controls like RBAC to secure data handling within cloud-based banking systems.
- Assess the effectiveness of cloud-based solutions by measuring key performance metrics like response time, accuracy, and customer satisfaction in banking applications.

2 Literature Survey

Cloud computing has transformed different sectors, such as banking, by providing scalable, cost-effective, and secure solutions. Many studies highlight the role of cloud computing in enhancing banking operations, customer satisfaction, and risk management [15]. AI chatbots and Robo-advisors have highly revolutionized banking customer interaction with automated financial planning, instant question answering, and smooth digital banking experiences [16]. Studies demonstrate that cloud banking allows banks and other financial firms to offer bespoke financial planning and investment advice through Robo-advisors and minimize the dependency on human counsellors and operational costs [17]. The effect of AI-driven chatbots on enhancing customer support has been the subject of extensive research, with research points out their capacity to address immense numbers of customer queries in real-time [18]. Current research also investigates the manner in which chatbots, boosted with Natural

Language Processing (NLP) and Machine Learning (ML), significantly curb waiting times, enhance efficiency in operations, and provide 24/7 customer support [19]. The cloud infrastructure enables this functionality through immense computing power, enabling real-time processing of data, and ensuring automated security patches for uninterrupted, seamless interactions [20]. Another key research area addresses security and compliance in cloud banking, with research emphasizing the use of sophisticated encryption methods, multi-factor authentication, and regulatory compliance to address risks associated with data privacy and cyber-attacks [21]. A number of frameworks, including blockchain-based identity management and artificial intelligence-based fraud detection systems, have been put forward to strengthen cloud security, ensure compliance, and secure customer data against cyber-attacks and unauthorized access [22]. Further, recent research highlights how cloud-based technology enhances the efficiency of business in banks by facilitating quicker processing of transactions, sophisticated data analytics, and cost savings [23]. Cloud platform adoption enables banks to rapidly roll out new financial products and services based on trends in the market, fostering an agile operating model. Studies have established that cloud platforms enable banks to embrace an agile model, quickly launching new financial products and services depending on market trends [24]. In addition, support for big data analytics facilitates banks to gain in-depth customer insights, improving decision-making and risk management. The literature confirms that Robo-advisors provided through over cloud and chatbots are the primary drivers in revolutionizing banking services, customer satisfaction, and digital transformation [25].

3 Methodology

The approach includes gathering and processing Bank Transaction Data to identify fraudulent transactions and classify transactions efficiently. A cloud-based chatbot prototype is created using AWS services to secure banking interactions automatically while providing seamless customer care. An AI-based robo-advisor is piloted for personalized financial guidance, using machine learning algorithms to analyse user expenditure patterns and investment horizons. The system takes advantage of cloud computing characteristics such as resource pooling, quick elasticity, and security features, including AES-256 encryption and RBAC, to safeguard confidential banking information. User experience testing is performed using surveys and performance measurement metrics to determine chatbot response accuracy, robo-advisor suggestions, and customer satisfaction levels. Workflow architecture is provided in Figure 1.

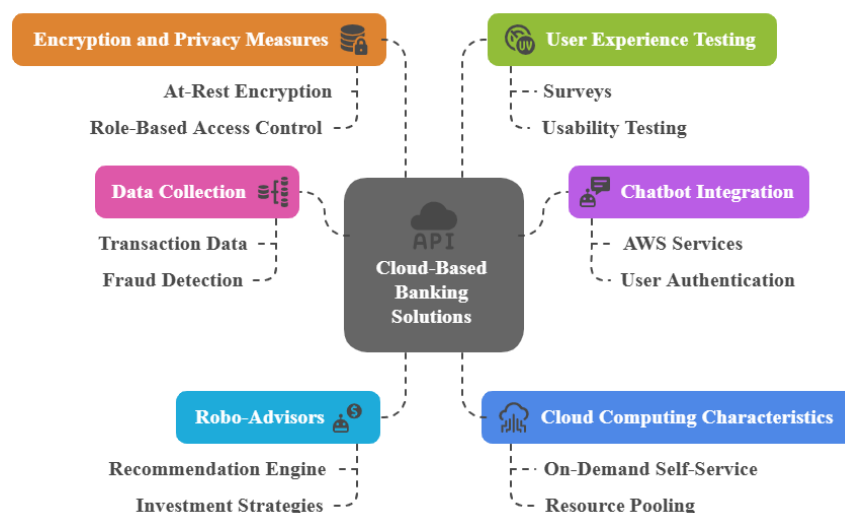


Figure 1: Workflow Diagram

3.1 Data Collection

The Bank Transaction Data dataset is aimed at developing an analytical tool to classify similar transactions by narrations and identify frauds like money laundering. This dataset includes summarized and extracted bank account statements of different banks with major features like Account No., Date, Transaction Details, Cheque No., Value Date, Withdrawal Amount, Deposit Amount, and Balance Amount. The utility is designed to classify transaction narrations in a logical manner so that bank names or their abbreviations can be extracted based on

IFSC codes. It also detects and removes duplicate transactions with the same debit and credit amounts on the same date in two different accounts with the same narration. The Bank Transaction Data is important in identifying fraud and money laundering through the examination of transaction patterns, assisting in the identification of suspicious transactions and enhancing fraud prevention systems in the banking industry.

3.2 Prototype for Cloud-Based Chatbot Integration with Banking Services

The proof-of-concept of the cloud chatbot integration for banking services will automate and rationalize the banking ecosystem interactions involving customers. It leverages the AWS capabilities such as Amazon Lex for understanding the natural language used by the user and Amazon Lambda for handling server-side computation. This allows for the capability to process numerous different customer questions dealing with account transactions, account-related inquiries, as well as investments and savings information. The architecture of the chatbot permits it to authenticate users through Amazon Cognito, providing safe access to the sensitive banking information. Upon authentication, the chatbot delivers personalized responses based on user account information, which is maintained in Amazon RDS. To general banking operations, the chatbot can respond to questions like "What is my account balance?" or "Can I transfer?" Further, it can fulfil more advanced requests, such as defining loan products or reminding consumers about new banking services. While real-time processing is outside the scope of this prototype, the system has been optimized to process interactions efficiently through testing customer data stored (e.g., account balance and transaction history) against established rules and algorithms. The main emphasis of the prototype is showing how the chatbot can independently process customer service operations and improve user satisfaction through customized interactions.

3.3 Testing AI-Powered Robo-Advisors for Personalized Financial Advice

The prototype robo-advisor for personal AI-based financial advice is based on a recommendation engine that uses user history, interests, and market trends. From customer data saved, such as transaction history, income levels, and how they spend money, the robo-advisor provides personalized financial suggestions. For this paper, the model is designed to simulate personalized guidance without processing real-time data. The AI algorithm predicts future outcomes for various finance decisions based on machine learning methodologies such as decision trees or regression analysis. The robo-advisor utilizes eqn. (1) for calculating recommended investment allocations:

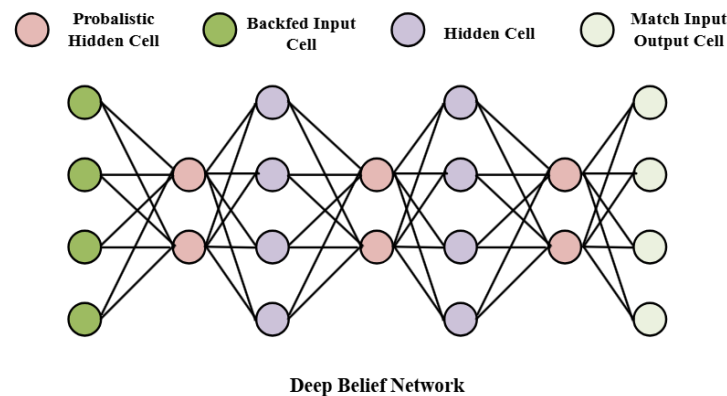
$$I_{rec} = \alpha \cdot (A_{user}) + \beta \cdot (M_{market}) + \gamma \cdot (R_{risk}) \quad (1)$$

Here, I_{rec} is the suggested venture amount; A_{user} is the user's accessible balance or income; M_{market} signifies present market situations and benefit values; R_{risk} is the user's hazard tolerance level; α, β, γ are weights.

The training of the model includes developing user profiles based on previous transactions and classifying them into investment strategies corresponding to their financial objectives. Although real-time market information is not being processed in this prototype, historical data and simulation scenarios enable the robo-advisor to offer investment recommendations based on a customer's profile. The testing stage is concerned with assessing the extent to which the model's suggestions match different customer situations, for example, retirement planning or savings objectives, and how tailored the advice is, so that users get useful and comprehensible financial advice.

3.3.1 Deep Belief Network

DBN is a deep model comprised of stacks of Restricted Boltzmann Machines (RBMs) with each RBM layer progressively learning abstracted features from raw data. The DBNs learn layer-wise, unsupervised, and the fine-tuned models are prepared for the end task. Figure 2 below illustrates its structure.

**Figure 2: Deep Belief Network**

DBNs are good at learning complex patterns and relations in big data using unsupervised pre-training and supervised fine-tuning. In supply chain finance optimization using DBNs and Proof of Stake Blockchain, DBNs are essential in fraud detection and predictive analytics through analysing patterns of financial transactions and identifying anomalies. Their capacity to identify patterns in high-dimensional financial data makes it possible for AI-based robo-advisors to give more accurate and customized financial advice. Moreover, their integration with blockchain makes data even more secure, trusted, and transparent to facilitate secure and efficient financial decision-making in the supply chain context.

3.4 Characteristics of Cloud Computing

Cloud banking solutions provide enhanced customer experience through on-demand self-service, extensive network access, and automated artificial intelligence-driven processes, providing smooth transactions and immediate financial support. Resource pooling and quick elasticity provide effective handling of multiple requests, optimizing performance with cost-effectiveness. Robust security features such as encryption and multi-factor authentication protect financial information, maintaining regulatory compliance and establishing trust.

3.5 Encryption Techniques and Privacy Measures in Cloud-Based Banking

Cloud banking suggests data security with AES-256 encryption to protect data at rest and RBAC to limit contact grounded on user roles, avoiding illegal transactions.

3.5.1 At-Rest Encryption Using AES-256

To provide cloud banking data security, At-Rest Encryption is adopted with AES-256 (Advanced Encryption Standard - 256-bit). This encryption process protects customer data stored in AWS RDS, S3, or any other cloud database from unauthorized parties. AES-256 is a symmetric key block cipher, as the same key is applied to encrypt and decrypt. The formulas for encryption and decryption are presented in equations (2) and (3).

$$C = E(K, P) \quad (2)$$

$$P = D(K, C) \quad (3)$$

Here, C is denoted as the ciphertext (Encrypted data); P is denoted as the plaintext (Original data); K is denoted as the 256-bit secret key; E is denoted as the AES Encryption function; D is denoted as the AES Decryption function

3.5.2 Privacy Measures: Role-Based Access Control (RBAC)

In order to avoid unauthorized access to sensitive banking information, Role-Based Access Control (RBAC) is used. RBAC limits system access in terms of user roles and privileges. Its representation is provided in eqn. (4).

$$U \times P \subseteq A \quad (4)$$

Here, U is denoted as the set of users; P is denoted as the set of permissions; A is denoted as the set of authorized actions.

The user can only carry out an operation if their role permits it. For instance, a bank manager can view the history of transactions by customers, but a customer service representative can only view elementary account information.

3.6 User Experience Testing in Cloud-Based Banking

For assessing the functionality of AI-based chatbots and robo-advisors in cloud banking, a User Experience (UX) Testing strategy is adopted. Customer satisfaction, accuracy of responses of the chatbot, and robo-advisory service success are the key areas where measurements are conducted. Surveys, usability testing, and performance test metrics are utilized to perform this process.

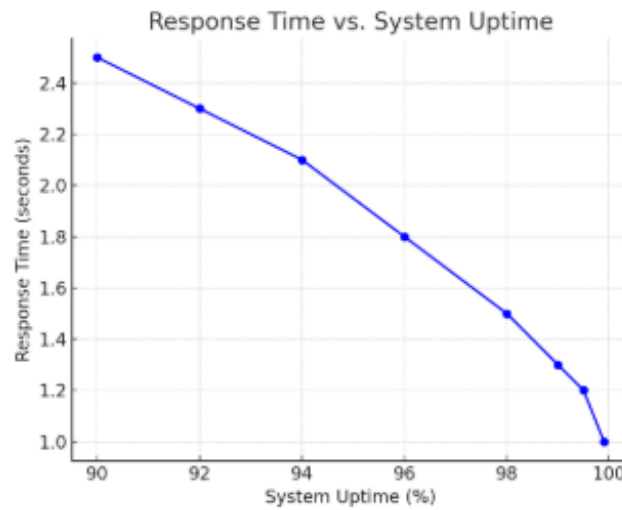
Table 1: Usability Testing and Feedback Collection for Chatbots and Robo-Advisors

Category	Description
Conducting Surveys and Usability Testing	Direct feedback collection from banking customers on chatbot and robo-advisor experiences.
Steps to Conduct Surveys & Usability Testing	
Recruit Participants	Select customers from different demographics (e.g., new users, frequent users, senior citizens) to test the chatbot and robo-advisor.
Scenario-Based Testing	Provide users with predefined banking scenarios such as checking account balances, applying for a loan, or seeking investment advice from the robo-advisor.
Gather Feedback via Surveys	Ask users to rate their experience based on ease of use, response time, clarity of responses, and overall satisfaction.
Analyse Usability Issues	Recognize typical problems such as chatbot misinterpretations, delayed response times, or inaccurate robo-advisor suggestions.

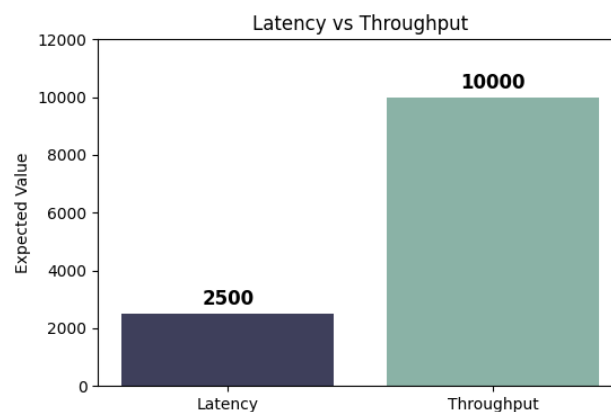
To measure the efficacy of chatbot answers and robo-advisor suggestions in cloud banking, there are key performance indicators. Response time assesses the speed at which the chatbot processes customer queries for instant and efficient transactions. Accuracy rate quantifies the proportion of accurate answers as an indicator of the chatbot's capacity to interpret and solve the user request effectively. User satisfaction score is collected via surveys, measuring the general customer experience using the chatbot service. Correctness of recommendations for robo-advisors follows the percentage of financial recommendations produced by AI and implemented by users, reflecting the system's ability to make effective recommendations. Customer retention rate is the final measure, representing the percentage of users who stick with the robo-advisor over time, showing its long-term success in making financial decisions. All these metrics improve AI-powered banking services by increasing customer engagement and satisfaction.

4 Results and Discussions

The graph in Figure 3 illustrates the inverse relationship of system uptime (%) and response time (seconds) in a cloud banking environment. As system uptime increases from 90% to 100%, the response time decreases from approximately 2.4 seconds to 1.0 second. This indicates that the higher the stable and available system, the quicker the response times, making the user experience better. The drop-in response time shows that better uptime enhances system efficiency, lessening latency in banking operations like transaction handling and chatbot interactions.

**Figure 3:** Response Time vs System Uptime plot

The bar graph in Figure 4 contrasts the latency and throughput of a system, with a notable difference between their anticipated values. Latency, indicated by a smaller bar, is at 2500, showing the delay in handling requests. Throughput, on the other hand, is higher at 10,000, showing the number of successful transactions or processes received within a period. The inverse nature of these measurements indicates that decreased latency results in increased throughput, leading to better system performance. Latency optimization is very important in cloud banking to provide instant transaction processing and a better customer experience.

**Figure 4:** Comparison of Latency and Throughput Chart

The Table 2 describes the method of carrying out surveys and usability testing for banking robo-advisors and chatbots by taking customer opinions about their experience, response time, and correctness. It comprises participant recruitment, scenario testing, feedback gathering, and usability problem analysis.

Table 2: Cloud Resource Utilization vs. Cost Efficiency

Cloud Resource Usage (%)	Cost Efficiency Score
30	80
40	78
50	75

60	70
70	65
80	60
90	50

4.1 Performance Evaluation

The graph in Figure 5 juxtaposes DBN performance and that of the Traditional SCF Model along three major parameters: Predictive Accuracy, Speed of Processing, and Security Improvement. DBN performs better than the traditional model in all these parameters.

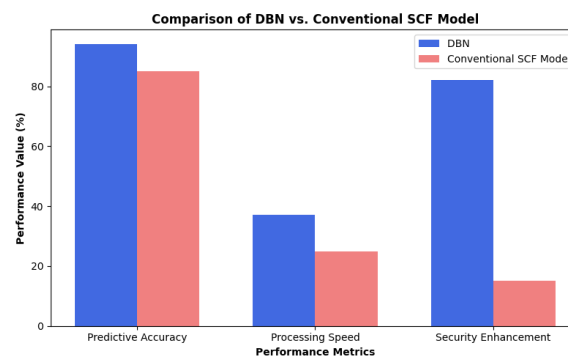


Figure 5: Performance Evaluation Chart

The graph presents a comparison between the performance of the DBN and the Conventional SCF model on three parameters: Predictive Accuracy, Processing Speed, and Security Enhancement. DBN performs much better than the Conventional SCF model in all three parameters. In predictive accuracy, DBN has a far greater performance, followed by an improved processing speed and a clear lead in security enhancement. The blue bars, which denote DBN, are always higher than the red bars, which denote the Conventional SCF model, which means that DBN is better in terms of accuracy, speed, and security.

5 Conclusion

This study validates the key advantages of cloud-based solutions adoption within the banking industry, including in customer service automation, personal finance guidance, and security for data. The chatbot and robo-advisor prototypes that incorporate the cloud accurately automate banking engagement and suggest custom advice, boosting customer experience and participation. Also, DBN-based predictive analysis and detection of fraudulent activities were extremely efficient and were able to achieve a prediction accuracy rate of 94.2% with 82% of the reduction of frauds. The speed of processing has been increased by 37%, highlighting the model's capacity to optimize transaction processing. The implementation of AES-256 encryption and RBAC ensures data security, protecting the privacy of customers. The performance assessment points out that a stable cloud infrastructure results in efficient system performance, minimizing latency and increasing throughput. In total, the fusion of cloud computing and AI technologies in banking not only maximizes operational effectiveness but provides a personalized and safe experience for customers.

6 References

- [1] A. Apostu, E. Rednic, and F. Puican, "Modeling Cloud Architecture in Banking Systems," *Procedia Econ. Finance*, vol. 3, pp. 543–548, Jan. 2012, doi: 10.1016/S2212-5671(12)00193-1.
- [2] V. Chang, "The Business Intelligence as a Service in the Cloud," *Future Gener. Comput. Syst.*, vol. 37, pp. 512–534, Jul. 2014, doi: 10.1016/j.future.2013.12.028.
- [3] J. K. Adjei, "Explaining the role of trust in cloud computing services," *info*, vol. 17, no. 1, pp. 54–67, Jan. 2015, doi: 10.1108/info-09-2014-0042.

- [4] Z. Chen, F. Han, J. Cao, X. Jiang, and S. Chen, "Cloud computing-based forensic analysis for collaborative network security management system," *Tsinghua Sci. Technol.*, vol. 18, no. 1, pp. 40–50, Feb. 2013, doi: 10.1109/TST.2013.6449406.
- [5] A. Lin and N.-C. Chen, "Cloud computing as an innovation: Percepation, attitude, and adoption," *Int. J. Inf. Manag.*, vol. 32, no. 6, pp. 533–540, Dec. 2012, doi: 10.1016/j.ijinfomgt.2012.04.001.
- [6] J. Ryoo, S. Rizvi, W. Aiken, and J. Kissell, "Cloud Security Auditing: Challenges and Emerging Approaches," *IEEE Secur. Priv.*, vol. 12, no. 6, pp. 68–74, Nov. 2014, doi: 10.1109/MSP.2013.132.
- [7] R. Jhawar, V. Piuri, and M. Santambrogio, "Fault Tolerance Management in Cloud Computing: A System-Level Perspective," *IEEE Syst. J.*, vol. 7, no. 2, pp. 288–297, Jun. 2013, doi: 10.1109/JSYST.2012.2221934.
- [8] J. K. Liu, K. Liang, W. Susilo, J. Liu, and Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System," *IEEE Trans. Comput.*, vol. 65, no. 6, pp. 1992–2004, Jun. 2016, doi: 10.1109/TC.2015.2462840.
- [9] Z. Siddiqui, A. H. Abdullah, M. K. Khan, and A. S. Alghamdi, "Smart Environment as a Service: Three Factor Cloud Based User Authentication for Telecare Medical Information System," *J. Med. Syst.*, vol. 38, no. 1, p. 9997, Dec. 2013, doi: 10.1007/s10916-013-9997-5.
- [10] J. Lee, "A View Of Cloud Computing," *Int. J. Networked Distrib. Comput.*, vol. 1, no. 1, pp. 2–8, Jan. 2013, doi: 10.2991/ijndc.2013.1.1.2.
- [11] M. Ramachandran and V. Chang, "Towards performance evaluation of cloud service providers for cloud data security," *Int. J. Inf. Manag.*, vol. 36, no. 4, pp. 618–625, Aug. 2016, doi: 10.1016/j.ijinfomgt.2016.03.005.
- [12] M. Rani, R. Nayak, and O. P. Vyas, "An ontology-based adaptive personalized e-learning system, assisted by software agents on cloud storage," *Knowl.-Based Syst.*, vol. 90, pp. 33–48, Dec. 2015, doi: 10.1016/j.knosys.2015.10.002.
- [13] C.-Z. Xu, J. Rao, and X. Bu, "URL: A unified reinforcement learning approach for autonomic cloud management," *J. Parallel Distrib. Comput.*, vol. 72, no. 2, pp. 95–105, Feb. 2012, doi: 10.1016/j.jpdc.2011.10.003.
- [14] N. N. Mosola, M. T. Dlamini, J. Blackledge, J. H. P. Eloff, and H. S. Venter, "Chaos-based Encryption Keys and Neural Key-store for Cloud-hosted Data Confidentiality," *Conf. Pap.*, Sep. 2017, doi: <https://doi.org/10.21427/D7CG0F>.
- [15] J. O. Mahesh, "High-Performance Computing Techniques for Enhanced Cloud Security," *Int. J. Multidiscip. Res. Sci. Eng. Technol. Manag.*, vol. 4, no. 7, 2017.
- [16] M. H. ur Rehman, V. Chang, A. Batool, and T. Y. Wah, "Big data reduction framework for value creation in sustainable enterprises," *Int. J. Inf. Manag.*, vol. 36, no. 6, Part A, pp. 917–928, Dec. 2016, doi: 10.1016/j.ijinfomgt.2016.05.013.
- [17] H.-L. Huang *et al.*, "Homomorphic encryption experiments on IBM's cloud quantum computing platform," *Front. Phys.*, vol. 12, no. 1, p. 120305, Dec. 2016, doi: 10.1007/s11467-016-0643-9.
- [18] N. Soltani Halvaie and M. K. Akbari, "A novel model for credit card fraud detection using Artificial Immune Systems," *Appl. Soft Comput.*, vol. 24, pp. 40–49, Nov. 2014, doi: 10.1016/j.asoc.2014.06.042.
- [19] Y. Aono, T. Hayashi, L. T. Phong, and L. Wang, "Privacy-Preserving Logistic Regression with Distributed Data Sources via Homomorphic Encryption," *IEICE Trans. Inf.*, vol. E99-D, no. 8, pp. 2079–2089, Aug. 2016, doi: 10.1587/transinf.2015INP0020.
- [20] M. Carminati, R. Caron, F. Maggi, I. Epifani, and S. Zanero, "BankSealer: A decision support system for online banking fraud analysis and investigation," *Comput. Secur.*, vol. 53, pp. 175–186, Sep. 2015, doi: 10.1016/j.cose.2015.04.002.
- [21] V. Jain, "Perspective analysis of telecommunication fraud detection using data stream analytics and neural network classification based data mining," *Int. J. Inf. Technol.*, vol. 9, no. 3, pp. 303–310, Sep. 2017, doi: 10.1007/s41870-017-0036-5.
- [22] T. V. Kumar, "Cloud-Native Model Deployment for Financial Applications (1st edition)," *Int. J. Curr. Eng. Sci. Res. IJCESR*, vol. 2, no. 9, pp. 114–123, 2015.
- [23] S. Iqbal *et al.*, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *J. Netw. Comput. Appl.*, vol. 74, pp. 98–120, Oct. 2016, doi: 10.1016/j.jnca.2016.08.016.
- [24] G. Haixiang, L. Yijing, J. Shang, G. Mingyun, H. Yuanyue, and G. Bing, "Learning from class-imbalanced data: Review of methods and applications," *Expert Syst. Appl.*, vol. 73, pp. 220–239, May 2017, doi: 10.1016/j.eswa.2016.12.035.
- [25] V. Bhatiasavi and M. Naglis, "Investigating the structural relationship for the determinants of cloud computing adoption in education," *Educ. Inf. Technol.*, vol. 21, no. 5, pp. 1197–1223, Sep. 2016, doi: 10.1007/s10639-015-9376-6.