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

An Intelligent AI-Enabled Cloud Security System for Certifying Information in Financial Sectors

Vishakha D. Bhandarkar[1*], M.P. Karthikeyan[2], Dr. Sadaf Hashmi[3], Dhiraj Singh[4], Syed Rashid Anwar[5], and Dr. Kirti Bikram[6]

[1*]Assistant Professor, Department of Applied Mathematics and Humanities, Yeshwantrao Chavan College of Engineering, India. vishakhabhandarkar@gmail.com, https://orcid.org/0000-0001-6998-5037

[2]Assistant Professor, Department of Computer Science and Information Technology, Jain (Deemed to be University), Bangalore, Karnataka, India. karthikeyan.mp@jainuniversity.ac.in, https://orcid.org/0000-0002-2346-0283

[3]Associate Professor, Department of ISME, ATLAS SkillTech University, Mumbai, Maharashtra, India. sadaf.hashmi@atlasuniversity.edu.in, https://orcid.org/0009-0008-8729-8423

[4]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. dhiraj.singh.orp@chitkara.edu.in, https://orcid.org/0000-0002-1710-0070

[5]Assistant Professor, Department of Computer Science & IT, ARKA JAIN University, Jamshedpur, Jharkhand, India. syed.r@arkajainuniversity.ac.in, https://orcid.org/0000-0001-9810-8850

[6]Assistant Professor, Assistant Professor, Symbiosis Law School, Pune (SLS-P), Symbiosis International (Deemed University) (SIU), Pune, India. kirti.bikram@symlaw.ac.in, https://orcid.org/0000-0002-4666-8271

Received: January 23, 2025; Revised: March 03, 2025; Accepted: April 17, 2025; Published: May 30, 2025

Abstract

Certifying information entails ensuring the correctness and validity of data. This procedure ensures that the information given is accurate and satisfies the requirements. Certification is performed by authorised persons, establishing confidence in the integrity of the information and increasing reliability for a variety of objectives. In this research, research aim is to develop an intelligent AI-enabled cloud security system for certifying information in the financial sector. This study's main focus is server-side data and compute security, which addresses the requirement for secure cloud data storage as well as additional safety precautions. Intelligent Seagull optimized ensemble Naive Bayes (ISO-ENB) has been utilised to choose the best appropriate available server for a particular job. Generally, homomorphic encryption is employed to ensure the integrity of the data that is communicated by encrypting the data before sending it to the server. The proposed model incorporates hill climbing refined Advanced Encryption Standard (HC-AES) with ISO-ENB to evaluate which server will be most profitable. Research evaluated the suggested model with various parameters such as data privacy ratio (91%), risk reduction ratio (99.1%) and scalability ratio (98%). The experimental outcomes illustrate the effectiveness of the recommended data security model.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 173-184.
DOI: *10.58346/JISIS.2025.I2.013*

*Corresponding author: Assistant Professor, Department of Applied Mathematics and Humanities, Yeshwantrao Chavan College of Engineering, India.

This system does provide secure mechanisms for sharing keys and backing up data, both of which are important in maintaining the privacy of sensitive data stored in the financial cloud infrastructure.

Keywords: Certifying Information, Cloud Security, Artificial Intelligence (AI), Hill Climbing Refined Advanced Encryption Standard (HC-AES), Financial Sectors, Intelligent Seagull Optimized Ensemble Naive Bayes (ISO-ENB).

1 Introduction

The phrase cloud computing refers to a new paradigm that has emerged for offering clients a range of digital services, such as servers, storage, software creation platforms and various platforms (Islam et al., 2023). The resources, apps and services in a cloud computing paradigm are created, deployed, and cloud security is ensured by high user authentication, encryption and data privacy standards when information in the financial industry is certified (Bharany et al., 2022). Multi-tenancy and cloud computing are crucial components to make an efficient use of the resources and initiatives that are present in effect. Several clients might be hosted by a single operating system, networked computer facility and server by using VMware; cloud providers serve an enormous number of users through the notion of resource sharing (Marques et al., 2020). The financial industry has seen a swift digital revolution in recent times, with cloud computing emerging as a critical technology propelling financial transaction records. Cloud services are a desirable option for financial institutions looking to update their operations that provide unmatched scalability, flexibility and affordability (Đurić & Topalić Marković, 2023). The banking sector has adopted cloud technology significantly as a result of innovation, agility and cost efficiencies in the financial sector and user authentication logs (Thulasi & Dharmaraj, 2025). Financial organizations such as banks, insurance providers, investment firms and others are moving their applications, data and infrastructure to cloud-based environments (Awotunde et al., 2021). Financial institutions demand information certification in cloud security to adhere to regulations, reassure clients' data protection protocols and maintain the integrity of their services (Meier et al., 2023). A third-party validation of security measures, risk management procedures and compliance with professional standard procedures is offered using certification (Riasanow et al., 2021). Figure 1 depicts the significant characteristics of cloud computing.

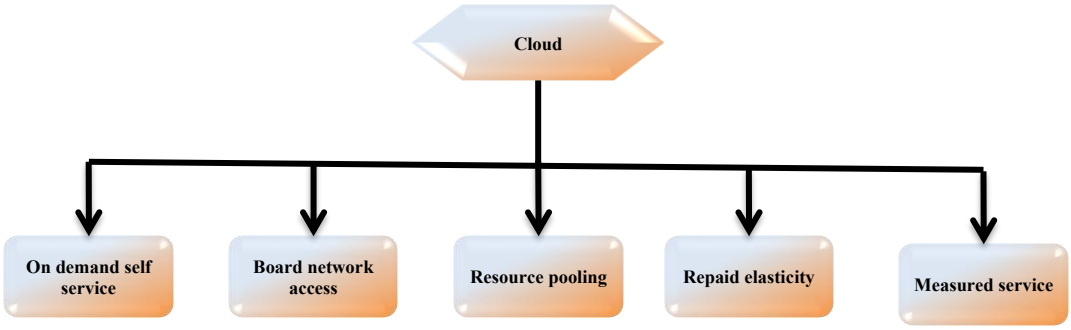

Figure 1: Significant Characteristics of Cloud Computing

Certification and Auditing by Third Parties

To evaluate and verify their cloud security posture, financial institutions use independent auditors (Mishchenko et al., 2021). SOC 2, PCI DSS and ISO 27001 certifications, among others, certify compliance with security requirements and provide stakeholders with security assurance.

Security Measures for Data and Encryption

Confidential financial data saved in the cloud is protected from intruders by using encryption methods, access restrictions and data loss prevention (DLP) technologies (Kafi & Akter, 2023). The potential risk of data breaches or unauthorized access caused by dependence on external cloud infrastructure, which creates vulnerabilities to direct organizational control, was one of the drawbacks of using a cloud security system for information certification in the financial sector (Clementine et al., 2014). This study aims to protect sensitive financial data that is transferred and stored on cloud devices. To enhance trust and dependability in the financial system by ensuring compliance with industry laws, eliminating illegal access, detecting threats and mitigating risks.

2 Related Work

Podrecca et al., (2022) examined the connection between obtaining the certification and businesses' profitability with a particular emphasis on the sector's largest widely used standard was ISO/IEC 27001. The results demonstrate that higher revenue growth, profitability and productivity of labor were associated with the international organization standardization (ISO) 27001 certification. The degree of globalization of the certified business indicates that it possesses an influence. Li et al., (2021) were examined in light of the data gathered from the questionnaires utilizing structural equation modelling (SEM). The standards' implementation was categorized as a preventative organizational innovation. The findings indicate that four important elements significantly impact consumer satisfaction while utilizing financial services: cloud services, safety, online instruction and service quality. Mirtsch et al., (2021) was explained to improve acquaintance with the use of an ISO/IEC 2700-based system for managing information security (Wan & Hu, 2024). SEM was used to identify the causes for the relatively low adoption of this control system standard in cloud organizations. Awadallah et al., (2021) described a blockchain-based cloud computing approach that assures privacy of information using homomorphic encryption techniques was proposed (Rahman & Begum, 2024). The selected cryptocurrency was the essential setup activity expected by the client for the method validation mechanism, which depended on public crypto, and was the background examination. The findings indicate that external verification is beneficial, and that public and private data might be used in place of each other when determining the cost of bank debt. Garg et al., (2021) were used to calculate the perceived business advantages of using blockchain technology in the banking sector, which offers measurements to assess the advantages. The early stages of blockchain-based technology might impact the outcomes with advancements and practical theoretical uses in its result highlighting its scientific and social value Shrivastava & Ahmed, (2024).

3 Dataset

The dataset comprises financial transaction records, network connection data, user authentication logs and security incident reports. It covers a range of circumstances, including effective login attempts, failed authentication attempts and abnormal activity. Financial domains for cloud security systems are thoroughly investigated using AI and validated using data from the banking, insurance and investment sectors.

4 Classification Method Using ISO-ENB

Financial industry, information is certified using the ISO-ENB procedure and leverages ensemble learning and ENB algorithms with the intelligence of seagulls to improve information certification procedures. Cloud computing has opened up a new, more reliable, adaptable and guarantee-filled environment for computation service customers and user authentication certification in the financial sector. The assortment data was server-side computation, and data security satisfies more safety requirements for secure cloud data storage. The security feature provided by the bidirectional authentication approach is shown graphically in Figure 2.

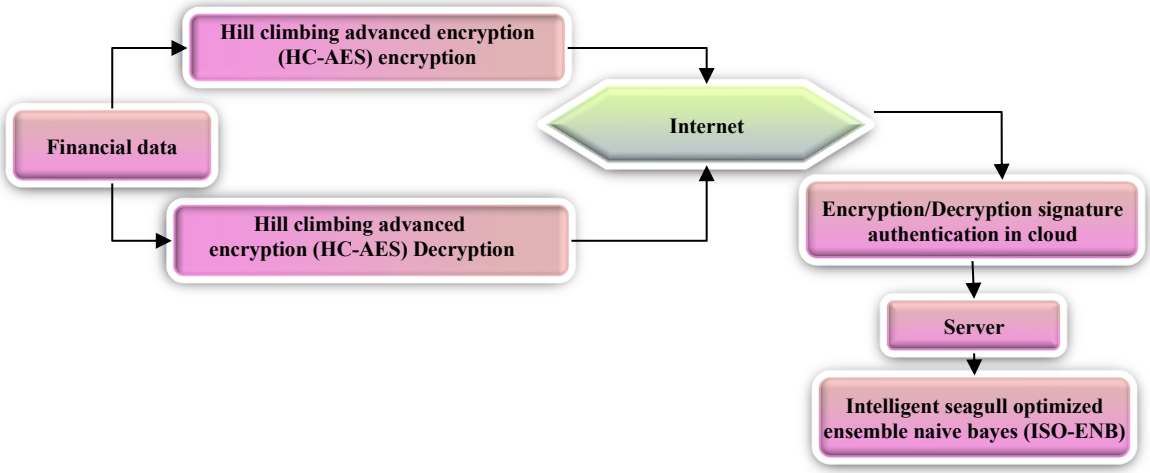

Figure 2: Proposed Flow Process

4.1 Intelligent Seagull Optimized (ISO)

An innovative metaheuristic algorithm called ISO was motivated by gull behavior, and the financial industry was used for information certification and provides effective solutions in the financial sector. To improve decision-making procedures and guarantee the stability and dependability of financial data certification, assortment data was server side ISO leverages the collective intelligence of seagulls. The propensity to migrate and attack is innate in seagulls. Migration is the seasonal movement of individuals across large distances. To prevent collisions during flight, seagulls begin their journey in distinct spatial zones. In the financial sector, SOA is a mathematical intelligent model of two behaviors that was created by continuously adjusting the seagull locations, an iterative search for the most suitable reaction to be conducted.

- **Stage of Migration**

A flock of seagulls moving from one place to another is represented by migration behaviors. The seagull was avoiding collision and moving in the direction of its best neighbour in the intelligent certifying stage and staying near the superior search agent. In the midst of migration, SOA mimics the action of seagulls as it alternates between locations. To avoid collisions with other seagulls, the measured seagull's value is increased by the variable Bas shown by equation (1).

$$\overrightarrow{O_M} = B \times \overrightarrow{O_d}(j) \quad (1)$$

The value of a non-colliding agent is denoted by $\overrightarrow{O_M}$ in equation (1), whereas the actual solutions at the ith phase are denoted by$\overrightarrow{O_d}$. B , is defined as follows and indicates the agent moving behavioruser authentication logs in the financial sector:

$$B = e_d - \left(j \times \left(\frac{e_d}{\max(j)} \right) \right) \quad (2)$$

The variable e_d in equation (2) represents B frequency control within the interval In the financial sector, the direction of the best option while effectively avoid collision with the seagull approach. The following is the description of this procedure in equation (3).

$$\overrightarrow{c_f} = A \times \left(\overrightarrow{O_a}(j) = \overrightarrow{O_d}(j) \right) \quad (3)$$

Wherec_f , financial sector initial point of O_d relative to O_a exploration and exploitation are regulated by B which is a random value indicated by the coefficient$A$using equation (4).

$$A = B^2 \times Q \times 2 \quad (4)$$

Q, was produced from O, C in this case, using equation (5) best agent is determined by the following algorithm, The ultimate step is changing the locations of the agents:

$$\overrightarrow{C_f} = \left| \overrightarrow{O_M} + \overrightarrow{C_f} \right| \quad (5)$$

Certifying information indicates the separation between the agent and the best agent financial sector is represented by C_f .

4.2 Ensemble Naive Bayes (ENB)

An effective method for boosting cloud security in the banking industry is ENB, which evaluates financial data user authentication. Ensuring the security and confidentiality of financial data is handled and stored in the cloud and using various ENB classifiers in an ensemble framework, ENB enhances classification accuracy and reliability, which strengthens the industry assurance and compliance. It might be used for text analysis and spam filtering. With numerous advantages, including simplicity of use, speed and effectiveness, ENB is regarded as one of the largest algorithms. ENB offers simple and highly advanced classification algorithms. The ENB theorem offers a method for computing posterior probability. The ENB theorem offers a method for deriving the posterior probability $(c \mid x)$ from $(x), (c)$, and $(c \mid x)$ using equation (6).

$$P(x \mid c) = \frac{P(c|x)}{P(x)P(c)} \quad (6)$$

The values of the equation are:

- The value of$(x \mid c)$, were antecedent chances for the group c It is a target that is given by the predictor. x characteristics.
- The values of $P(c)$It is a group of previous chances in poster probability.
- The value of $(c \mid x)$Is the estimated value of the prediction assigned to a class in certified use data in the financial sector?
- The value of $P\ (c)$ was a predictor of antecedent certainty.

4.3 Hybrid of ISO-ENB

Intelligent algorithms such as the ISO-ENB are used by an effective cloud authentication system to certify financial data assortment data stored on the server side. The method is to improve the safety records of the financial industry and protect essential data from cyberattacks.

4.4 Encrypt and Decrypt the Data Using Hill Climbing Refined Advanced Encryption Standard (HC-AES)

Financial sectors are assured of reliable data safety using HC-AES, an effective encryption standard enhanced with hill climbing improvement. It encrypts essential information using cloud security approaches, rendering it imperceptible to unauthorized users. The identical approach is used in decryption, which protects financial data from security breaches and ensures confidentiality and integrity for every transaction and procedure. Initially, each transaction of data in the population is a global search that was built based on information transmitted to the sense units. Second step, a local search is conducted using the information individual to each effective unit and enhances the data location of user authentication logsand HC-AES is the foundation of regional search in the financial sector. A heuristic optimization approach called HC-AES might enhance the way of finance industry uses HC-AES. Financial organizations are communicating securely across networks by using HC-AES, which protects private data from interception and monitoring. Financial information is certified by cloud security substances that use the HC-AES AES as an essential component. Secure data is protected from unwanted access and modification by strong encryption provided by HC-AES. The confidentiality, integrity, and validity of financial transactions and assortment data are ensured by HC-AES when it is used inside cloud infrastructures. Random symmetric key is a security measure that reassures financial data users that their sensitive information is protected, as its adoption in the banking industry demonstrates a dedication to advanced security measures. Figure 3 shows the flow of HC-AES.

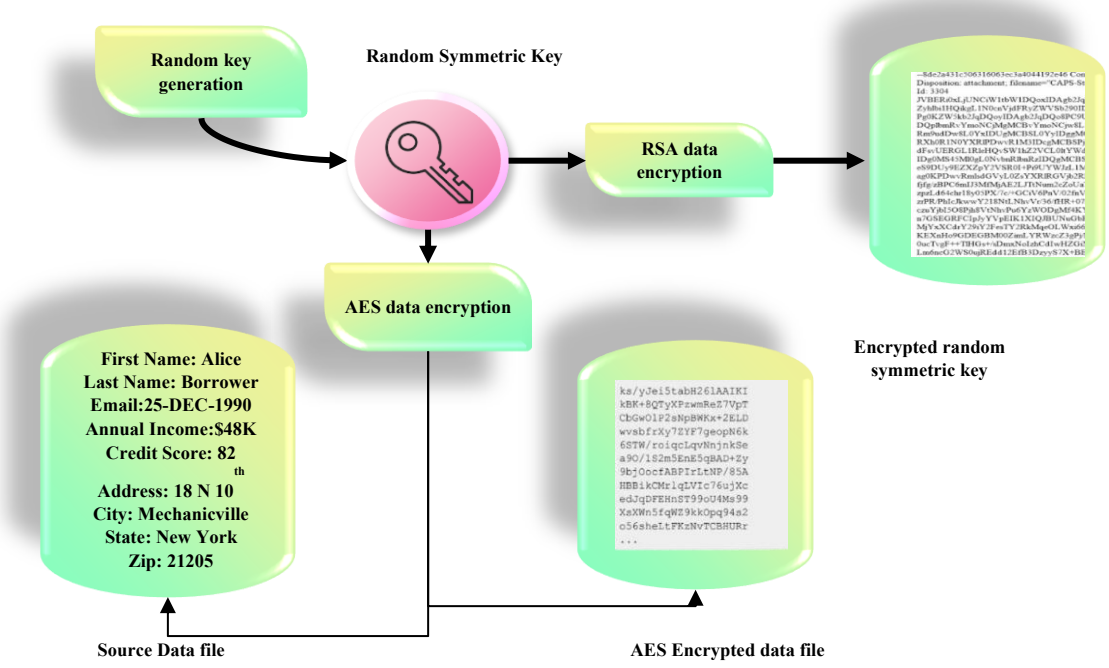

Figure 3: Workflow of Encrypted Financial Data

5 Results and Discussion

To evaluate the financial data of the suggested method in terms of scalability, risk reduction ratio, data privacy and existing methods such as support vector machine (SVM) (Mishra, 2023), k-nearest neighbour (KNN) (Mishra, 2023), is explained in detail.

- **Risk Reduction Ratio**

Data confidentiality and integrity are vitally dependent on the risk reduction ratio when it comes to cloud security certification for financial data. The financial industry might improve confidence in cloud-based systems and protect confidential data by providing strong certification mechanisms in place that reduce the risk of illegal access, data breaches and regulatory non-compliance. The risk reduction ratio comparative analysis using proposed and existing approaches is shown in Figure 4, and Table 1 denotes the numerical outcomes of the risk reduction ratio. When compared to other existing approach, our proposed ISO-ENB achieves 99.1% and existing methods such as SVM attains 79.5%, KNN attains 98.7%. It demonstrates the greater efficiency of our proposed approach than other existing methods.

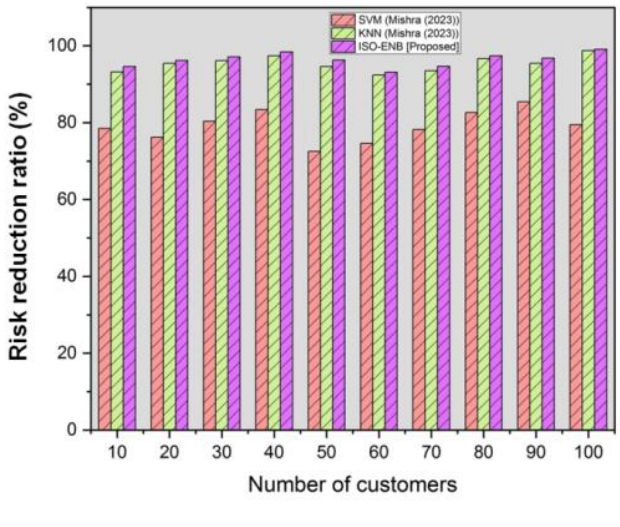

Figure 4: Result of Risk Reduction Ratio

Table 1: Numerical Outcomes of Risk Reduction Ratio

Number of customers	Risk reduction ratio		
	SVM (Mishra, 2023)	KNN (Mishra, 2023)	ISO-ENB (Proposed)
10	78.5	93.2	94.6
20	76.2	95.4	96.2
30	80.4	96.1	97.1
40	83.4	97.4	98.4
50	72.5	94.6	96.3
60	74.6	92.4	93.1
70	78.2	93.5	94.7
80	82.6	96.7	97.4
90	85.4	95.4	96.8
100	79.5	98.7	99.1

- **Interpretation of the Scalability Ratio**

Scalability is the ability to manage growing data volumes, user demands and system complexities in an effective way while preserving robust safety precautions that are modified to the particular requirements and laws of the financial industry in a cloud-based security system for financial information certification. The scalability ratio comparative analysis using proposed and existing approaches is shown in Figure 5, and Table 2 denotes the numerical outcomes of the scalability ratio. When compared to other existing approach, our proposed method, ISO-ENB achieves 98.4% and existing methods such as SVM attains 72%, KNN attains 94%. It demonstrates the greater efficiency of our proposed approach better than other existing methods.

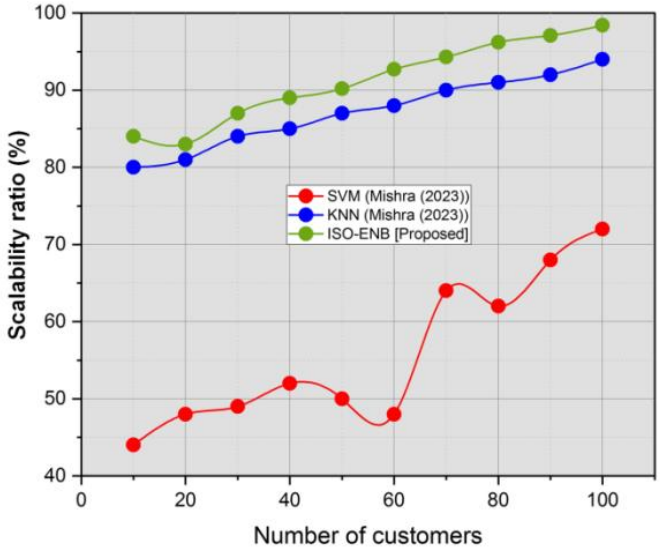

Figure 5: Result of Scalability

Table 2: Numerical Comparison of Scalability

Number of customers	Scalability ratio (%)		
	SVM (Mishra, 2023)	KNN (Mishra, 2023)	ISO-ENB (Proposed)
10	44	80	84
20	48	81	83
30	49	84	87
40	52	85	89
50	50	87	90.2
60	48	88	92.7
70	64	90	94.3
80	62	91	96.2
90	68	92	97.1
100	72	94	98.4

- **Data Privacy Ratio**

Financial information in cloud security must be certified by an efficient data privacy and security system. Encryption, access restrictions, coupled with routine assistance to protect sensitive data from cyber

threats and illegal access by ensuring its confidentiality, integrity, as well as availability. The data privacy ratio comparative analysis using proposed and existing approaches is shown in Figure 6, and Table 3 denotes the numerical outcomes of the privacy ratio. When compared to other existing approaches, the ISO-ENB method achieves 91% and existing methods such as SVM attain 63%, KNN attains 81%. It demonstrates that the greater efficiency of the proposed approach is greater than other existing methods.

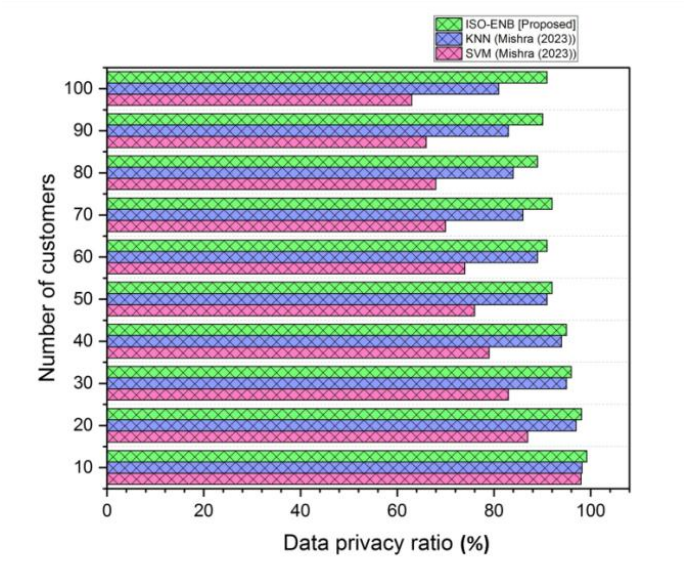

Figure 6: Result of Data Privacy Ratio

Table 3: Numerical Outcomes of Data Privacy Ratio

Number of customers	**Data privacy ratio (%)**		
	SVM (Mishra, 2023)	KNN (Mishra, 2023)	ISO-ENB (Proposed)
10	98	98.2	99.2
20	87	97	98.1
30	83	95	96
40	79	94	95
50	76	91	92
60	74	89	91
70	70	86	92
80	68	84	89
90	66	83	90.1
100	63	81	91

6 Conclusion

The innovative qualities of cloud computing were scalability and the ability to drastically cut down on data storage costs, and assortment order on the server side, which can increase computational power by a large number of user-authenticated data in financial sectors. Problems with regulatory compliance, reliability of data, verification procedures and the need for uniform standards across various institutions represent a few of the issues that have occurred during information certification in the financial industry. To overcome this problem, research proposed the ISO-ENB method in cloud security systems for

certifying information in financial sectors is to protect sensitive financial data that is transferred and stored in cloud devices. To enhance trust and dependability in the financial system by ensuring compliance with industry laws, eliminating illegal access, detecting threats and mitigating risks. Our experiment results, notably, data privacy ratio achieved 91%, the risk reduction ratio achieved 99.1%, scalability ratio achieved 98%, which shows that our proposed ISO-ENB approach produces the risk reduction ratio with outstanding results. The proneness of the method to erroneous classifications through the feature independence assumption is a disadvantage of deploying a cloud security system for information certification in the financial sector. In the future, improved digitization, real-time detection of threats, adaptive learning and compatibility with modern technologies, including blockchain, will be the possible features of an AI-powered cloud security system for information certification in the financial sectors.

References

[1] Awadallah, R., Samsudin, A., Teh, J. S., & Almazrooie, M. (2021). An integrated architecture for maintaining security in cloud computing based on blockchain. *IEEE Access, 9,* 69513-69526. https://doi.org/10.1109/ACCESS.2021.3077123

[2] Awotunde, J. B., Adeniyi, E. A., Ogundokun, R. O., & Ayo, F. E. (2021). Application of big data with fintech in financial services. In Fintech with artificial intelligence, big data, and blockchain (pp. 107-132). *Singapore: Springer Singapore.* https://doi.org/10.1007/978-981-33-6137-9_3

[3] Bharany, S., Kaur, K., Badotra, S., Rani, S., Kavita, Wozniak, M., ... & Ijaz, M. F. (2022). Efficient middleware for the portability of paas services consuming applications among heterogeneous clouds. *Sensors, 22*(13), 5013. https://doi.org/10.3390/s22135013

[4] Đurić, D., & Topalić Marković, J. (2023). Eco Tourism Development based on Natural and Artificial Surroundings in Semberija and Majevica Area. *Archives for Technical Sciences, 1*(28), 69–76. https://doi.org/10.59456/afts.2023.1528.069Dj

[5] Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., & Modgil, S. (2021). Measuring the perceived benefits of implementing blockchain technology in the banking sector. *Technological forecasting and social change, 163,* 120407. https://doi.org/10.1016/j.techfore.2020.120407

[6] Islam, R., Patamsetti, V., Gadhi, A., Gondu, R. M., Bandaru, C. M., Kesani, S. C., & Abiona, O. (2023). The future of cloud computing: benefits and challenges. *International Journal of Communications, Network and System Sciences, 16*(4), 53-65. https://doi.org/10.4236/ijcns.2023.164004

[7] Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy, 10*(1), 15-26.

[8] Li, F., Lu, H., Hou, M., Cui, K., & Darbandi, M. (2021). Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technology in Society, 64,* 101487. https://doi.org/10.1016/j.techsoc.2020.101487

[9] Marques, R. P., Santos, C., & Duarte, R. (2020, June). Promotion of Accountability and Performance of the Social Economy Entities with SaaS Multi-Tenant Information Systems. *In 2020 15th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE. https://doi.org/10.23919/CISTI49556.2020.9140813

[10] Meier, H. B., Marthinsen, J. E., Gantenbein, P. A., & Weber, S. S. (2023). Financial digitalization, FinTech, and the collaborative economy. In Swiss Finance: Banking, Finance, and Digitalization (pp. 527-548). *Cham: Springer International Publishing.* https://doi.org/10.1007/978-3-031-23194-0_11

[11] Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & security, 109,* 102383. https://doi.org/10.1016/j.cose.2021.102383
[12] Mishchenko, S., Naumenkova, S., Mishchenko, V., & Dorofeiev, D. (2021). Innovation risk management in financial institutions. *Investment Management and Financial Innovations, 18*(1), 191-203. http://dx.doi.org/10.21511/imfi.18(1).2021.16
[13] Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences, 13*(10), 5875. https://doi.org/10.3390/app13105875
[14] Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry, 142,* 103744. https://doi.org/10.1016/j.compind.2022.103744
[15] Rahman, S., & Begum, A. (2024). Analysis of Structural Integrity in High-Rise Buildings Under Dynamic Load Conditions Using AI: A Computational Perspective. *Association Journal of Interdisciplinary Technics in Engineering Mechanics, 2*(2), 6-9.
[16] Riasanow, T., Jäntgen, L., Hermes, S., Böhm, M., & Krcmar, H. (2021). Core, intertwined, and ecosystem-specific clusters in platform ecosystems: analyzing similarities in the digital transformation of the automotive, blockchain, financial, insurance and IIoT industry. *Electronic Markets, 31*(1), 89-104. https://doi.org/10.1007/s12525-020-00407-6
[17] Shrivastava, V., & Ahmed, M. (2024). The Function of the Blockchain System in Enhancing Financial Integrity and the Confidence of Society. *Global Perspectives in Management, 2*(4), 36-45.
[18] Thulasi, A. R., & Dharmaraj, A. (2025). A Study on Awareness Towards Corporate Governance and its Dimensions Among the Microfinance Institutions. *Indian Journal of Information Sources and Services, 15*(1), 244–251. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.31
[19] Wan, Q., & Hu, X. (2024). Legal Framework for Security of Organ Transplant Information in the Digital Age with Biotechnology. *Natural and Engineering Sciences, 9*(2), 73-93. https://doi.org/10.28978/nesciences.1569190
[20] Yogesha, T., & Thimmaraju, S. N. (2025). Development of a Lexicon for Manets to Enhance Performance and Security. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 16*(1), 362-374. https://doi.org/10.58346/JOWUA.2025.I1.022

Authors Biography

Vishakha D. Bhandarkar is an Assistant Professor in the Department of Applied Mathematics and Humanities at Yeshwantrao Chavan College of Engineering, India. She specializes in applied mathematics and interdisciplinary studies that support engineering education. Vishakha is actively involved in teaching, research, and academic development.

M.P. Karthikeyan is an Assistant Professor in the Department of Computer Science and Information Technology at Jain (Deemed-to-be University), Bangalore, Karnataka, India. His research interests include software engineering, data analytics, and artificial intelligence. He is actively engaged in teaching, research, and student mentoring in emerging computing technologies.

Dr. Sadaf Hashmi is an Associate Professor in the Department of ISME at ATLAS SkillTech University, Mumbai, Maharashtra, India. Her expertise lies in strategic management, innovation, and entrepreneurship. She is actively involved in research, teaching, and fostering industry-academia collaboration.

Dhiraj Singh is associated with the Centre of Research Impact and Outcome at Chitkara University, Rajpura, Punjab, India. He focuses on enhancing research quality, impact assessment, and promoting collaborative academic initiatives. Dhiraj is actively involved in supporting institutional research strategies and knowledge dissemination.

Syed Rashid Anwar is an Assistant Professor in the Department of Computer Science & IT at ARKA JAIN University, Jamshedpur, Jharkhand, India. His research interests include cybersecurity, network security, and information technology. He is actively involved in academic teaching, research, and student mentoring.

Dr. Kirti Bikram is an Assistant Professor at Symbiosis Law School, Pune (SLS-P), Symbiosis International (Deemed University), Pune, India. Her academic expertise includes legal studies, human rights, and constitutional law. Dr. Bikram is actively engaged in research, teaching, and contributing to legal scholarship.