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

# Advanced Cloud Security System with Cryptography-Based Three-Layer Authentication for Banking Services

Dr. Ved Prakash Mishra[1*], Narmadha Thangarasu[2], Dr. Hemal Thakker[3], Simranjeet Nanda[4], Sneha Kashyap[5], and Dr. Shibani C Aich[6]

[1*]Associate Professor, Department of Computer Science and Engineering, Amity University Dubai, UAE. mishra.ved@gmail.com, https://orcid.org/0000-0003-1832-8736

[2]Assistant Professor, Department of Computer Science Engineering, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Bangalore, Karnataka, India. narmadha.t@jainuniversity.ac.in, https://orcid.org/0000-0001-9628-4236

[3]Assistant Professor, Department of ISME, ATLAS Skill Tech University, Mumbai, Maharashtra, India. hemal.thakker@atlasuniversity.edu.in, https://orcid.org/0009-0002-0043-5760

[4]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. simranjeet.nanda.orp@chitkara.edu.in, https://orcid.org/0009-0005-6893-8585

[5]Assistant Professor, Department of Computer Science & IT, ARKA JAIN University, Jamshedpur, Jharkhand, India. sneha.k@arkajainuniversity.ac.in, https://orcid.org/0000-0003-0276-9449

[6]Department of English, Amrita Vishwa Vidyapeetham, Amrita Puri, India. shibaniaich@gmail.com, https://orcid.org/0000-0001-9304-2207

Received: July 23, 2025; Revised: September 05, 2025; Accepted: October 09, 2025; Published: November 28, 2025

## Abstract

The ability to store data on a cloud server for scalable services was made possible by cloud computing. To collect cloud user data from many locations using wireless means, IoT includes dispersed sensor nodes. However, the authentication time wasn't reduced, and the accuracy of the authentication did not increase. An IoT framework with three-layer authentication known as the Adaptive Elgamal Cryptosystem Algorithm (AECA) Three-Layer Authentication Method is proposed to overcome these problems. Initially, we collected a Kaggle dataset. The dataset's target parameter includes details on ten thousand bank clients. Of these, 2037 samples belonged to the class of negativity, and 7963 samples belonged to the category of the positive category. The AECA Method aims to facilitate efficient IoT financial transactions with a higher level of confidentiality. It involves a cloud user as the buyer and a cloud server as the seller, with the Cloud Server generating public and private keys during the key generation phase. When a user needs to make a financial transaction, they use a key pair to log in and send a demand message to customer support. The cloud manipulator is considered and authorized when the user's password and fingerprint match the computer system's password. If not, the transaction is rejected. The study encryption time (13.64), decryption time (15.28), Key generation time (347.21) and security (94), considering variations in

*Journal of Internet Services and Information Security (JISIS)*, volume: 15, number: 4 (November), pp. 243-253.
DOI: *10.58346/JISIS.2025.I4.018*

*Corresponding author: Associate Professor, Department of Computer Science and Engineering, Amity University Dubai, UAE.

financial data entries and cloud users. By using the AECA Method, this strategy makes it possible to execute financial transactions quickly and securely.

**Keywords**: Financial Transaction, Authentication, Internet of Things (IoT), Adaptive Elgamal Cryptosystem Algorithm (AECA).

# 1 Introduction

Modern research is beginning to focus on security in cloud computing. With online storage replacing conventional information storage, the majority of organizations are adopting novel procedures (Kumar et al., 2021). It provides effective access to information at any time from any location (Hossain & Al Hasan, 2022).

Simulations using cloud computing are conventional for the great majority of applications. Cloud-based availability is attracting everyone to store data, as access to surrounding rings can be problematic (Hossain & Hasan, 2022). The cloud is accessible everywhere. Through a cloud server that provides overpowering computational capacity is also economical, cloud computing enables asset clumsy clients to comprehend their massive computational remaining duties at hand (Ouma et al., 2024).

The rapid growth of cloud computing technology has completely changed how companies run and handle their data (Li et al., 2021). The banking sector, which is very concerned about security and data that has realized the potential advantages of implementing cloud computing technologies (Balaji et al., 2023). Banks can increase their operational efficacy, scalability and cost-effectiveness with the help of cloud computing. However, security worries continue to be a major barrier to cloud computing's mainstream adoption in the banking industry. Because of the scalability, flexibility and cost-effectiveness constraints of traditional IT infrastructures, banks are looking into cloud computing solutions (Alemami et al., 2023).

By providing banks with on-demand access to shared computing resources, cloud computing allows them to optimize their operations and concentrate on their main business of banking (Adee & Mouratidis, 2022; Alzubi et al., 2022). Banking clients have more access to their bank accounts via the Internet and mobile devices because of the information technology industry's explosive growth. While e-banking arrives in several forms, its primary differentiators are the financial data processing methods, hardware and software that are accessible (Udayakumar et al., 2023). The study aims to present the Adaptive Elgamal Cryptosystem Algorithm (AECA) (Almaliki & Al-saedi, 2023). Performing IoT-based, efficient financial transactions with a greater rate of confidentiality is the primary goal of the AECA Method (Ishak et al., 2025) (Boopathy et al., 2025). The study is divided into four parts (Darapour, 2016). The related work is included in part 2 (Shrivastava & Ahmed, 2024). The methods are explained in depth in Part 3. Part 4 provides findings of the study. A conclusion is provided in Part 5 (Gaba et al., 2024).

# 2 Related Work

Thabit et al., (2023) assessed security algorithms by contrasting their robustness and efficiency with their computational expense. Lightweight-blocking cryptography, stream encryption and hybrid ciphers are covered in the study. Therefore, estimates and studies indicated that by 2020, there will be more than 50 billion connected gadgets. The study concluded by outlining IoT security risks, assaults and methods to mitigate vulnerabilities.

Gupta et al., (2022) suggested a novel population theory-driven verification method for IoV security that was made possible by blockchain technology. The approach was a three-layer multi-trusted authorization system offered here, enabling instantaneous vehicle identification from the initial point of entry to the areas under the control of various believed officials. It was accomplished through the use of "Physical Unclonable Functions (PUFs)" initially, followed by duel gaming and a "dynamic Proof-of-Work (dPoW)" consensus mechanism.

Alzubi et al., (2022) presented a novel technique for defensive the discretion of electronic medical archives by combining "deep learning (DL)" and blockchain technologies. CNN was used to classify regular and deviant operators from the processed dataset. The model performed and produced identification outcomes that were superior to those of other methods currently in use, according to experimental data obtained from simulations conducted using the Python programming tool.

Mohammed et al., (2023) investigated that a reliable decentralized system for authentication can be constructed using the technology of Blockchain (Samyadevi et al., 2024). By employing a digital ledger model to strengthen the resilience of periodic verification on the information by utilizing an optimized number of obtained bioacoustics indicate included instead of traditional biometric traits for authorization, maximum safety for the bioacoustics indicator authentication system was ensured (Vignesh et al., 2023).

Gaba et al., (2024) provided a "Blockchain-enabled Fog networking environment security architecture (B-SAFE)" for connected vehicles. Initially, as a preliminary to the structure, blockchain safety and automotive fog communication were presented. Secondly, a three-layer architecture for B-SAFE was introduced, with an emphasis on cloud-based trust and incentive administration for automobiles, cryptocurrency at fog nodes and automotive communications. Thirdly, a procedure and diagrams were provided, together with information about how the blockchain was being implemented at fog nodes.

Mohanta et al., (2022) examined various privacy and security issues in IoT applications. Second, research was conducted on blockchain technology, offering a solution for certain IoT security issues. A smart transport network uses the consensus technique PBFT, which depends on the blockchain system, to carry out safe computations. Vulnerability research demonstrated that even in the presence of malfunctioning or malevolent nodes in the suggested protocol operated as intended.

Obaidat et al., (2020) offered a thorough classification of IoT threats, utilizing the three-layer design framework. It also suggested these attacks may affect CIA missions in relevant products by examining the sense, system and software tiers. In addition, the research suggested defences and reductions by adopting a multifaceted approach as opposed to a single-layer approach.

Gharavi et al., (2024) examined the various PQC kinds and their newly introduced standardized basics in the survey to see whether they can provide security for blockchain-based IoT applications. Additionally, it covered new suggestions for blockchain-IoT applications, and it gave a quick introduction to blockchain.

# 3 Methodology

A framework for cloud computing is being established to improve the safety of financial data transactions. The AECA Method structure is shown in Figure.1 with cloud users and a cloud server for the exchange of financial data. The suggested AECA Method's structure diagram for safe cloud data transactions is described in Figure.1. Users of the cloud $CU_1, CU_2, CU_3 \ldots.. CU_n$ With financial data $fd_1, fd_2, fd_3, \ldots . fd_m$ is securely stored on the cloud server (CS) Registration, encryption, authentication, and decryption are all part of the AEC Method. The ensuing sections provide descriptions of the three AECA Method processes.

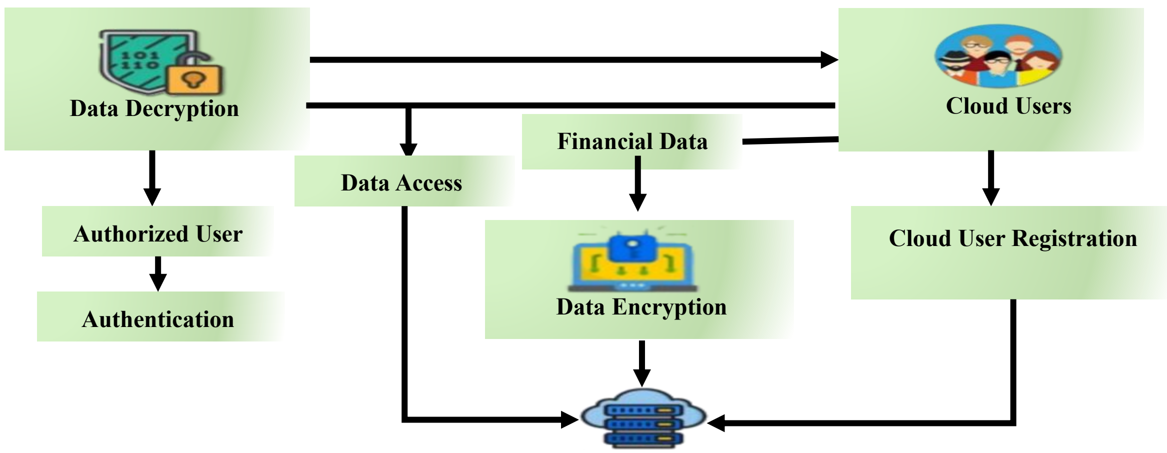


Figure 1: A framework design for the suggested AECA methodology

### 3.1 Dataset

The dataset, which was used to model churns was acquired via Kaggle. An integer parameter that shows whether a client has departed the bank or remains a client makes up the target parameter of the dataset, which encompasses information on 10,000 bank clients. In 2037 were negative class (exited) samples and 7963 were positive class (kept) samples. The binary flags 1 and 0 indicate the client's bank account is closed or retained, respectively, in the target variable. Thirteen feature vectors, or predictors, are included in the dataset, which were derived from consumer transactions and data (Rahman and Kumar 2020).

### 3.2 Adaptive Elgamal Cryptosystem Algorithm (AECA) based Three Layer Authentication

A new approach called the AECA Method has been presented to improve data privacy in cloud environments. In the AECA Technique, public key cryptography is used. AEC refers to the encryption keys that are generated at random for a specific duration. The AECA Method prevents unauthorized users from accessing data.

#### 3.2.1 Registration

The suggested AECA approaches preserve the data after first registering information with a cloud server. To secure a sizable amount of cloud user data on the cloud server, it's time to assume that a financial data transaction has been completed. Every cloud user has been registered by the cloud server. Names such as original, middle, last, birthdate, gender, contact, age, monthly income, weight, etc., are collected by the cloud manipulator during the registration procedure. After the registration procedure, each registered user receives a key pair from the cloud server.

A huge prime number $o$ should be chosen such that $\frac{o-1}{2}$ is also prime. $M$ is the total amount of bits. Select alpha $< o$ as the base. Select $b < o$ for the private key.

Calculate $alpha^b\ (mod\ o)\ = beta$. Create two huge, randomized primes, $q\ and\ t$, that are nearly the same size and that are reduced by 4 produce a balance of 3. Subtract $m$ from$q^*t$. The extended Euclidean algorithm can be used to identify numbers B and A such that $B^*q + A^*t = 1$ . During the key generating stage, it is possible to determine B and A once and for all. Publicize keys $o, m, alpha, and\ beta$ while keeping private keys $B, A, b, q, and\ t$ a secret.

### 3.2.2 AECA Encryption

Data encryption, as used in the AECA Method, is an approach to encrypting financial data while it is sent from one location to another. Furthermore, the data is encrypted when it is allocated to the cloud server. Thus, the AECA Method was employed to ensure enhanced security on cloud servers. An asymmetric key cryptography algorithm that has a public and private key is called AECA. The recipient's public key is used for encryption to prevent unauthorized access to financial data.

Divide the data into $M - 1$ bit sections and fill them as needed. Choose a secret random number $l$ with $gcd\ l\ \ (l, o - 1)$. Every financial data block should have the same $l$. Determine the encryption key $f(w, l) = (z_1, z_2)$for each block $w$, where $z_1 = alpha^l(mod\ o)$ and $z_2 = beta^l w(mod\ o)$. The data blocks $z_1$ and $z_2$have a length of M. Ten continuous five ("5") digits should be added at the end of both$z_1$ and $z_2$, and $z_1$ and $z_2$ should be added as follows: $n = z_1 + (10\ consecutive$ "5" $digits)\ +\ z_2 +\ (10\ consecutive$ "5" $digits)$. Subtract $d$ from $n^2(mod\ m)$. D is the financial information.

### 3.2.3 Bivariate Coefficient Authentication

Cloud users must authenticate the authenticity of any data they need to access from the server. When the cloud server receives a request, it uses an AEC password to verify the user's validity.

The user authentication procedure in the cloud is shown in Figure. 2. The user messages the server with a request. Upon receiving the request, the server sends the AEC password (PIN). The user is regarded as having the appropriate authorization and is allowed to access the data from the server in the cloud, provided the password they entered (PIN) matches the password that the cloud server sent. A bivariate coefficient has been used to match an AEC password to a fingerprint. An AEC password and fingerprint are validated using a similarity indicator called the bivariate coefficient. One calculates the bivariate correlation as

$$BC = \frac{\sum x * x_i}{\sqrt{\sum x^2 \sum x_i^2}} \tag{1}$$

The bivariate similarity coefficient is indicated by "$BC$" in equation (1), the amount of product of the balancing score of two session passwords is represented by $\Sigma X * Xi$, the squared score of $X$ is implied by $\Sigma X2$, and the squared score of $Xi$ is indicated by $\Sigma Xi2$. The value of the bivariate correlation coefficient (X-coefficient) ranges from '+1' to '-1'. When there is a '+1' similarity coefficient, it means that the password and fingerprint have matched correctly, and the user is considered authorized to make financial transactions. If not, the financial transaction is refused, and the person is labeled as unauthorized.

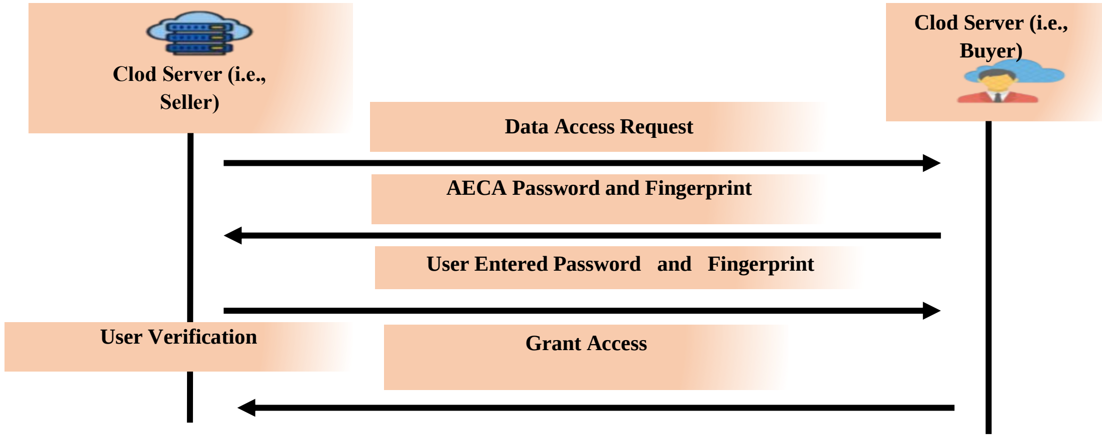


Figure 2: Procedure for authentication

### 3.2.4 AECA Decryption

After completing user authentication, the authorized handler obtains the original patient data and performs AECA decryption. With the use of a private key that the encryption has been completed.

Subtract $s_1$ from $d^{(q+1)/4} mod\, q$. Subtract $s_2$ from $d^{(t+1)4} mod\, t$. $mod\, m$, calculate $w = (B^* q^* s_2 + A^* t^* s_1) mod\, m$. Subtract $z$ from( $B^* q^* s_2 + A^* t^* s_1) mod\, m$. We obtain four sets of data, $n_1$ $n_2$ $n_3$ $n_4$, using $w$ and $z$ in the following ways: $n_1 = w, n_2 = -w, n_3 = z$, and $n_4 = -z$. Creating use of the additional sequential bytes that have been added to the final portion of the initial information$m$, we may determine that the four original data points are (original data m). Currently, we may find the data as follows by using the message $m$

We use the superfluous sequential bits inserted at the end of $z_1$ to partition the financial data $m$ into two subblocks, $z_1$ *and* $z_2$. Find the solution to calculate $w = z_2 (z_1^{b-1})(mod\ o)$for double consecutive blocks, $z_1$ *and* $z_2$. The desired block of data is $w$.

## 4 Results

The AECA uses innovative encryption approaches to improve cloud security. It optimizes the encryption and decryption procedures are implemented using Python's security package. RAM of 8GB is suggested for optimal cloud data security performance.

This section examines the "encryption time (s), decryption time (s), key generation time (ms), and security metrics. The classification performance of the fully homomorphic encryption (FHE), Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA) models is evaluated (Almalawi et al., 2024).

A cloud security system's "encryption time (s)" is the quantity of period desirable to encrypt the information before it is transmitted or stored, ensuring its privacy and security. It can be described as equation (2): the product of the data size (D), the complexity of the encryption algorithm (C) and the processing time per unit of data (T). The encryption time of FHE (36.33), AES (47.68), RSA (21.54) and AECA (13.64). The encryption time of the AECA Method has consequently enhanced (Figure.3).

$$Encryption\ time\ (s) = D * C * T \quad (2)$$

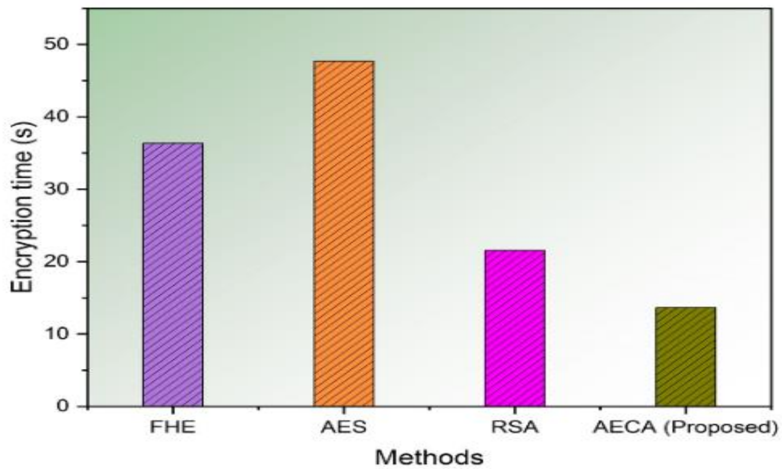


Figure 3: Encryption time

A cloud security system's "decryption time" (s) is the amount of time it takes to decode encrypted data. It is determined by variables like computational capacity (C), key size (K), and encryption method difficulty (E). It is represented as follows: equation (3). The decryption time of FHE (26.43), AES (45.76), RSA (26.43) and AECA (15.28). The decryption time of the AECA Method has consequently improved (Figure.4).

$$Decryption\ time\ (s)\ =\ E\ *\ K\ /\ C \tag{3}$$

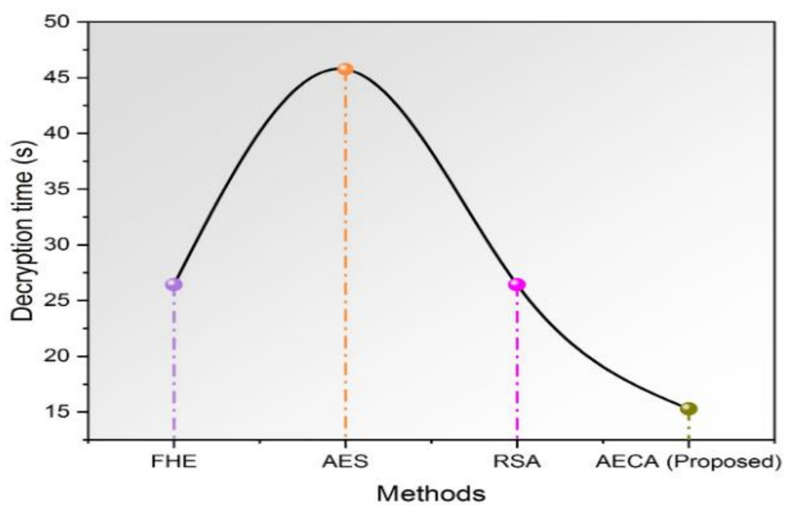


Figure 4: Decryption time

In a cloud security system, “key generation time (s)” is the quantity of period needed to generate keys that guarantee safe communication. It is influenced by variables including processing power (P), randomness generation (R), and algorithm complexity (C), which are described in equation (4). The key generation time of FHE (612.54), AES (873.76), RSA (569.34), and AECA (347.21). Consequently, the AECA Method's key generation time gets better (Figure 5).

$$Key\ generation\ time\ (s) = \frac{C \times R}{p} \tag{4}$$

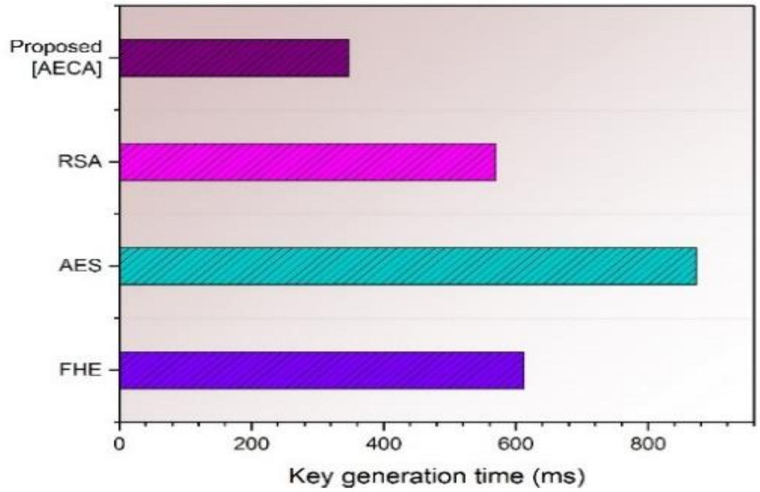


Figure 5: Key generation time

A cloud security system protects resources and data stored in cloud settings from cyber threats, illegal access and data breaches. The security of FHE (88%), AES (81%), RSA (92%), and AECA (94%). When compared to existing approaches, the AECA Method's security is higher and subsequently improved (Figure.6).

$$Cloud\ Security = Data\ Encryption + Access\ Control + Threat\ Detection \quad (5)$$

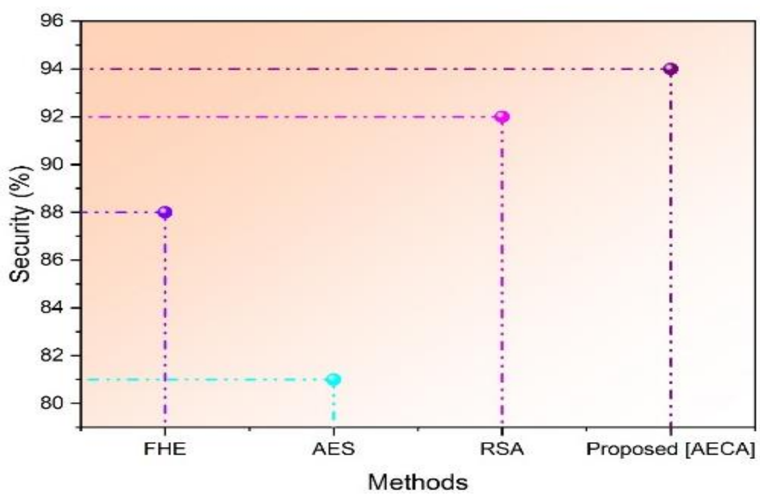


Figure 6: Security

Table 1 displays the overall numerical outcomes of the Evaluation metrics.

Table 1: Values of existing and proposed methods

| Methods | Encryption time (s) | Decryption time(s) | Key generation time (ms) | Security (%) |
|---|---|---|---|---|
| FHE | 36.33 | 26.43 | 612.54 | 88 |
| AES | 47.68 | 45.76 | 873.76 | 81 |
| RSA | 21.54 | 26.43 | 569.34 | 92 |
| AECA[Proposed] | 13.64 | 15.28 | 347.21 | 94 |

# 5 Conclusion

Enhancing the safety of financial data transfer in a cloud setting is the goal of the special AECA Method. This study used the AECA Method to complete the registration process. The key pair for the enumerated user is generated by the cloud server. The cloud user logs in and sends a request message to customer service when they need to complete any financial transactions. Afterwards, the Cloud server sends the password and fingerprint to verify the legitimacy of the cloud manipulator. The user is a registered user, and they can conduct financial transactions if the cloud manipulator inputs their password and their fingerprint matches the password that CS sent. The transaction will be declined in any other case. An effective secured financial transaction with higher data security and integrity is completed and utilizing the AECA Method. Finally, clouds are used to evaluate the combination of the encryption time (13.64), decryption time (15.28), Key generation time (347.21) and security (94%) of the proposed AECA Method in comparison with existing research. This method enables efficient and secure financial transaction execution by utilizing the AECA Method. The effectiveness of AECA depends on accurate adaptation processes, which may add computing complexity. Issues related to compatibility with current systems and weaknesses in key management could impede the smooth execution and dependability of operations. AECA can provide increased security in dynamic digital settings by adjusting to counteract changing threats related to cryptography. Sensitive data can be safeguarded across diverse platforms, due to its ability to adapt the evolving circumstances.

# References


[1] Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *22*(3), 1109.https://doi.org/10.3390/s22031109

[2] Alemami, Y., Al-Ghonmein, A. M., Al-Moghrabi, K. G., & Mohamed, M. A. (2023). Cloud data security and various cryptographic algorithms. *International Journal of Electrical and Computer Engineering*, *13*(2), http://doi.org/10.11591/ijece.v13i2.pp1867-1879

[3] Almalawi, A., Hassan, S., Fahad, A., & Khan, A. I. (2024). A hybrid cryptographic mechanism for secure data transmission in edge AI networks. *International Journal of Computational Intelligence Systems*, *17*(1), 24.https://doi.org/10.1007/s44196-024-00417-8

[4] Almaliki, O. J., & Al-saedi, M. O. (2023). The Impact of the Qualitative Peculiarities of Accounting Information Based on the Financial Reports of Commercial Banks. *International Academic Journal of Social Sciences*, *10*(1), 49-56. https://doi.org/10.9756/IAJSS/V10I1/IAJSS1006

[5] Alzubi, J. A., Alzubi, O. A., Singh, A., & Ramachandran, M. (2022). Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning. *IEEE Transactions on Industrial Informatics*, *19*(1), 1080-1087. https://doi.org/10.1109/TII.2022.3189170

[6] Balaji, R., Deepakkumar, A., Prabhu, G., Thinakaran, P., & Gowtham, S. (2023). Enhancing Network Security by using SDN Algorithm in Cloud Computing. *International Academic Journal of Science and Engineering*, *10*(1), 14–19. https://doi.org/10.9756/IAJSE/V10I1/IAJSE1003

[7] Boopathy, E. V., Niranjana, M. I., Prasath, S., Sivabalvigneshan, P., Sanjesh, R., Sanjay, S., ... & Vishal, S. (2025). Aegis Flare: IOT-Enabled Robotic Firefighter for Advanced Fire Detection and Suppression. *Archives for Technical Sciences/Arhiv za Tehnicke Nauke*, (32). https://doi.org/10.70102/afts.2025.1732.066

[8] Choudhary, K., Gupta, K., Chawla, R., Sharma, P., & Sharma, M. (2020). Cloud Computing Service Models: Traditional and User-Centric Approaches. *Applications of Cloud Computing*, 43-67.

[9] 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.

[10] Gaba, P., Raw, R. S., Kaiwartya, O., & Aljaidi, M. (2024). B-safe: Blockchain-enabled security architecture for connected vehicle fog environment. *Sensors*, *24*(5), 1515. https://doi.org/10.3390/s24051515

[11] Gharavi, H., Granjal, J., & Monteiro, E. (2024). Post-quantum blockchain security for the Internet of Things: Survey and research directions. *IEEE Communications Surveys & Tutorials*, *26*(3), 1748-1774. https://doi.org/10.1109/COMST.2024.3355222

[12] Gupta, M., Kumar, R., Shekhar, S., Sharma, B., Patel, R. B., Jain, S., ... & Iwendi, C. (2022). Game theory-based authentication framework to secure internet of vehicles with blockchain. *Sensors*, *22*(14), 5119. https://doi.org/10.3390/s22145119

[13] Hossain, M. A., & Al Hasan, M. A. (2022). Improving cloud data security through hybrid verification technique based on biometrics and encryption system. *International Journal of Computers and Applications*, *44*(5), 455-464. https://doi.org/10.1080/1206212X.2020.1809177

[14] Ishak, Z., Abidin, S., & Manaf, N. A. A. (2025). Cultivating change: Examining the influence of financial management courses on the financial practices of asnaf. *Indian Journal of Information Sources and Services*, *15*(1), 357-365. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.46

[15] Kumar, S., Karnani, G., Gaur, M. S., & Mishra, A. (2021, April). Cloud security using hybrid cryptography algorithms. In *2021 2nd international conference on intelligent engineering and management (ICIEM)* (pp. 599-604). IEEE. https://doi.org/10.1109/ICIEM51511.2021.9445377

[16] 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

[17] Mohammed, Z. H., Chankaew, K., Vallabhuni, R. R., Sonawane, V. R., & Ambala, S. (2023). Blockchain-enabled bioacoustics signal authentication for cloud-based electronic medical records. *Measurement: Sensors*, *26*, 100706. https://doi.org/10.1016/j.measen.2023.100706

[18] Mohanta, B. K., Samal, K., Jena, D., Ramasubbareddy, S., & Karuppiah, M. (2022). Blockchain-based consensus algorithm for solving security issues in distributed internet of things. *International Journal of Electronic Business*, *17*(3), 283-304. https://doi.org/10.1504/IJEB.2022.124331

[19] Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. (2020). A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers*, *9*(2), 44. https://doi.org/10.3390/computers9020044

[20] Ouma, Geoffrey, Mzee Awuor, Kanyi Patrick Wamuyu, and Bernard Maake. "Designing a comprehensive framework for data and network security in cloud computing: case of Kenyan banking industry." *African Journal of Emerging Issues* 6, no. 2 (2024): 24-45.

[21] Rahman, M., & Kumar, V. (2020, November). Machine learning based customer churn prediction in banking. In *2020 4th international conference on electronics, communication and aerospace technology (ICECA)* (pp. 1196-1201). IEEE. http://dx.doi.org/10.1109/ICECA49313.2020.9297529

[22] Samyadevi, V., Anguraj, S., Singaravel, G., & Suganya, S. (2024). Image Based Authentication Using Zero-Knowledge Protocol. *International Academic Journal of Innovative Research*, *11*(1), 01–05. https://doi.org/10.9756/IAJIR/V11I1/IAJIR1101

[23] 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.

[24] Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography algorithms for enhancing IoT security. *Internet of Things*, *22*, 100759. https://doi.org/10.1016/j.iot.2023.100759

[25] Vignesh, S., Prasanth, N., & Vasanth, P. (2023). Authentication by Graphical Password Using Digital Signature Algorithms. *International Journal of Advances in Engineering and Emerging Technology*, *14*(1), 130-132.


## Authors Biography

**Dr. Ved Prakash Mishra** is an Associate Professor in the Department of Computer Science and Engineering at Amity University Dubai, UAE. His research interests span artificial intelligence, cybersecurity, and data analytics. He has authored numerous publications and is actively involved in academic research and student development.

**Narmadha Thangarasu** is an Assistant Professor in the Department of Computer Science Engineering at the Faculty of Engineering and Technology, Jain (Deemed-to-be University), Bangalore, Karnataka, India. Her areas of interest include artificial intelligence, software engineering, and data science. She is actively engaged in teaching, research, and student mentorship.

**Dr. Hemal Thakker** is an Assistant Professor in the Department of ISME at ATLAS SkillTech University, Mumbai, Maharashtra, India. She specializes in management education with a focus on innovation, entrepreneurship, and strategic leadership. Dr. Thakker is actively involved in research, curriculum development, and student engagement.

**Simranjeet Nanda** is associated with the Centre of Research Impact and Outcome at Chitkara University, Rajpura, Punjab, India. He is focused on promoting research excellence, enhancing scholarly communication, and fostering impactful academic collaborations. His work supports institutional research strategies and knowledge dissemination.

**Sneha Kashyap** is an Assistant Professor in the Department of Computer Science & IT at ARKA JAIN University, Jamshedpur, Jharkhand, India. Her academic interests include software development, database systems, and emerging technologies in computer science. She is actively involved in teaching, research, and academic mentoring.

**Dr. Shibani C. Aich** is a faculty member in the Department of English at Amrita Vishwa Vidyapeetham, Amritapuri, India. Her academic interests lie in literature, cultural studies, and interdisciplinary research in the humanities. She is committed to advancing critical thinking and scholarly inquiry through her teaching and publications.