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

Enhancing Credit Card Data Security Using AI-integrated Encryption and Tokenization Framework

Dr. Dipti N. Kashyap[1*], Dr. Kshitij Naikade[2], Dr. Arvind Kumar Pandey[3], Dr. Nittin Sharma[4], Dr. Sadaf Hashmi[5], and Dr. Sachin S. Pund[6]

[1*]Assistant Professor, Department of Mechanical Engineering, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India. diptikashyap22@gmail.com, https://orcid.org/0000-0003-4364-3121

[2]Assistant Professor, Symbiosis Law School, Pune (SLS-P), Symbiosis International (Deemed University) (SIU), Pune, India. kshitij.naikade@symlaw.ac.in, https://orcid.org/0000-0002-8307-1167

[3]Associate Professor, Department of Computer Science & IT, ARKA JAIN University, Jamshedpur, Jharkhand, India. dr.arvind@arkajainuniversity.ac.in, https://orcid.org/0000-0001-5294-0190

[4]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. nittin.sharma.orp@chitkara.edu.in, https://orcid.org/0009-0007-9740-8414

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

[6]Assistant Professor, Mechanical Engineering, Ramdeobaba University, RBU, Nagpur, Maharashtra, India. pundss@rknec.edu, https://orcid.org/0000-0002-5616-2469

Received: December 06, 2024; Revised: January 15, 2025; Accepted: January 30, 2025; Published: February 28, 2025

Abstract

In an age dominated by the rapid advancement of digital transactions, safeguarding sensitive financial information in cloud computing, particularly credit card data, has become increasingly crucial. Traditional security measures in financial cloud computing have shown weaknesses in ensuring the confidentiality, privacy and integrity of data, leaving unencrypted information vulnerable to unauthorized access and exposure. This paper introduces an innovative method called Tokenized Elliptic-Homomorphic Cryptography (TE-HC) which improves the financial information security in cloud computing. Additionally, Artificial Intelligence (AI) is integrated to detect whether the data is normal or potentially intrusive in financial information. Consisting of merchant and tokenization modules along with a token vault, the system enables secure transmission and validation of credit card details. Implemented results demonstrate its effectiveness, speed, while comparative analyses showcase its superior performance in credit card security. Overall, TE-HC offers enhanced security, efficiency and user experience, presenting a compelling solution to the critical challenges of protecting credit card data in the digital age.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 1 (February), pp. 316-329. DOI: *10.58346/JISIS.2025.I1.020*

*Corresponding author: Assistant Professor, Department of Mechanical Engineering, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India.

Keywords: Credit Card, Financial, Tokenized Elliptic-Homomorphic Cryptography (TE-HC), Artificial Intelligence (AI), Security, Cloud Computing.

1 Introduction

The quantity of Internet users has increased as a result of the Information Technology (IT) industry's recent rapid expansion. Internet access has given people around the world and has an excellent chance to communicate and enjoy life better. Additionally, it has given credit card companies and financial companies fresh motivation to expand into untapped markets and generate development prospects for the economy (Carrasco et al., 2020). Receiving credit card payments entails providing the merchant with pertinent data, like the card number, payment amount, expiration date and so on, before submitting to the Payment Gateway (PG), it should be verified (Campos, 2024). The processor receives the financial details provided by the PG and links up with the client's financial institution to determine to forward or deny the inquiry (Roseline et al., 2022; Rakesh et al., 2024). Instead of payment being transmitted right away to the merchant's bank, a digital payment token for a certified transaction a merchant's electronic payment information is given. The growth of Internet-based companies has been primarily described to consumers' increased trust in the company, as well as the degree to which data security in financial cloud computing may be upheld (Gamini et al., 202; Rabet & Mousavi, 2017). However, given the increasing range of theft, fraud, difficulties, and loss of service attacks on the financial data, users have expressed grave worries, uncertainties and loss of faith surrounding credit card information relocation, confidentiality, honesty and privacy in financial cloud computing (Shrivastava & Ahmed, 2024). Millions of dollars have been lost every year as a result of security flaws in both old and current credit card platforms that have been made vulnerable by intrusion, theft of data and other attacks in financial data (Sreeja et al., 2018). Due to security holes in both older and newer credit card networks that have been exposed by hacking, data theft and other attacks, millions of money have been lost annually (Cherif et al., 2024). Credit card fraud about merchants can take two forms: triangulation, wherein thieves use legitimate credit card details and customer information to order goods from a reputable website, or collusion, wherein the retailer and/or staff collaborate to perpetrate fraud by exploiting the customers' account information and/or personal information (Noviandy et al., 2023). The risks of credit card fraud are frequently shared by the cardholder, who might not be aware of the attack and the retailer. While retailers incur lost sales due to payback fees and the possibility of account deletion or suspension, cardholders face the difficult task of having a fraudulent payment reversed(Chakraborty et al., 2023).This paper introduces an innovative method called Tokenized Elliptic-Homomorphic Cryptography (TE-HC) which improves the financial information security in cloud computing. Additionally, Artificial Intelligence (AI) is integrated to detect the data is normal or potentially intrusive in financial information (Uvarajan, 2024; Maurya et al., 2025).

The following sections comprise the study, Section 2 includes the relevant works, and Section 3 outlines the methodology. The experimental results of the study are shown in section 4. There is a conclusion in section 5.

2 Related Works

Strelcenia & Prakoonwit, (2023) introduced a knowledge-based Conditional Generative Adversarial Network) K-CGAN, a novel data augmentation technique, to identify scams involving credit cards and looks into several techniques for data augmentation to deal with the issue of inconsistent data. These results show the superior Precision and Recall when compared to other approaches.

Taha & Malebary, (2020) proposed a method that effectively detects credit card scams by using an optimized light gradient boosting machine (OLightGBM). When the proposed strategy was compared to other ways employing the two sources of data, it generated the best results with a F1-score, accuracy, precision and the area of the operating characteristic of the receiver curve.

Alenzi & Aljehane, (2020) suggested that the method uses logistic regression to develop the classifier to prevent financial credit card transaction fraud. The two widely used classifiers, regarding precision, sensitivity and mistake frequency, the proposed classifier outperforms both the support vector machine and voting classifiers.

Tokenization was an additional database system security strategy suggested by Agboola et al., (2022) that involved replacing or substituting personal information with a token. The findings indicate that, in comparison to other security solutions, the tokenization technique has a high ability to secure sensitive data in cloud computing.

A security measure tokenization was the foundation of the strategy presented by Petrus (2023). A working prototype of the proposed strategy was created. The findings indicate that tokenization may eventually take the role of conventional encryption methods for cloud-based BI data security.

Ileberi et al., (2021) developed a machine learning (ML) based identity theft solution by using actual uneven data sets obtained from European credit merchants. Furthermore, the enhanced models produced better outcomes than the existing techniques.

Jayanthi et al., (2023) suggested ML can lessen the burden on financial institutions by assisting in the detection of fraudulent use of credit cards in transactions. The suggested method's performance was compared with the existing method and outperformed the other methods.

Habibpour et al., (2023) presented three uncertainty quantification (UQ) approaches for card fraud prediction. Demonstrate through research findings that the ensemble performs better at capturing insecurity related to providing forecasts.

Kuttiyappan & Rajasekar (2024) suggested three AI-based methods for fraud detection are presented. The effectiveness of the AI-powered methods was contrasted with random forest models, logistic regression and conventional rule-based systems. A thorough analysis was conducted to understand whether the new AI-based techniques are better at identifying fraudulent activity.

Duan et al., (2024) presented a new approach to the identification of fraudulent use of credit cards. Our results demonstrated the possibility of combining neural networks with graphs and causal reasoning to enhance the detection of fraud in monetary transactions.

3 Proposed System

Initially we gather dataset from Kaggle which shows the credit card transaction dataset that includes both valid and fraudulent transactions. From the data intrusive detection can be detected using ν -Support Vector Classification (ν -SVC). From the detection shows the data is intrusive reject and normal is consider for the merchant and tokenization module and the data is stored in cloud. Figure 1 shows the overview of the methodology.

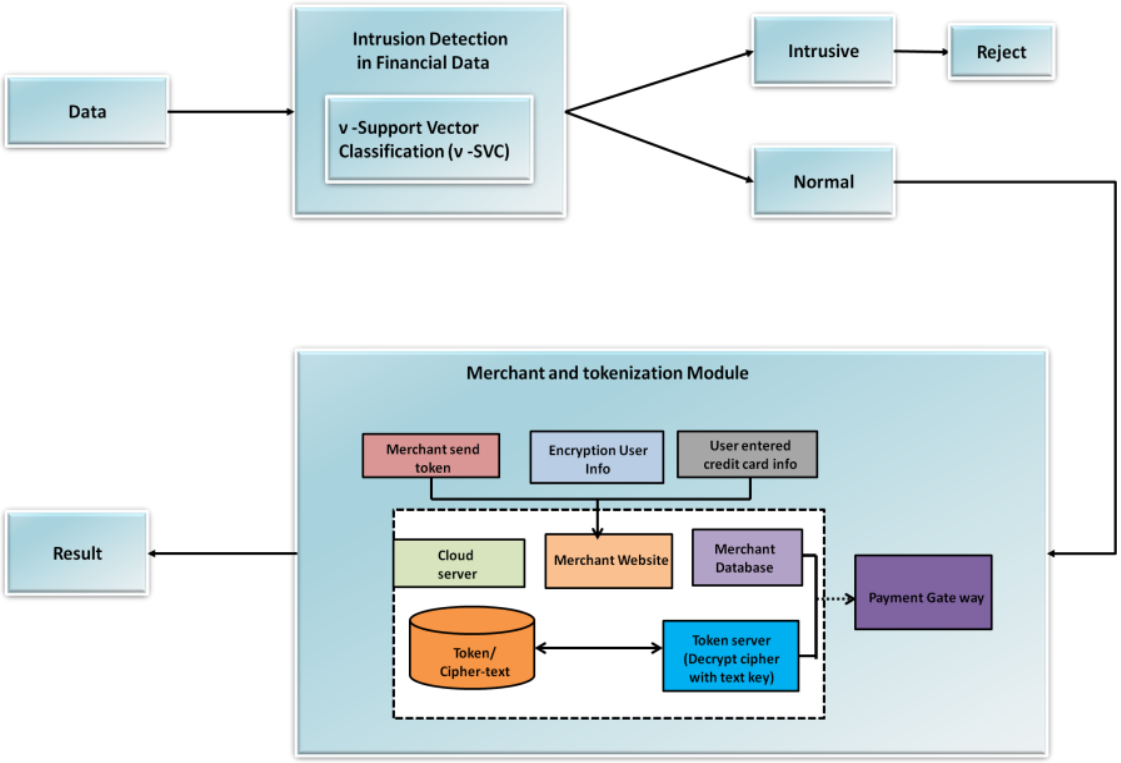


Figure 1: Overview of Methodology

3.1. Intrusive Detection

To detect the intrusive in credit card information using ν -Support Vector Classification (ν -SVC). A binary classification scenario is n-support vector classification (n-SVC). As there is nopriori way for choosing parameter C in$C - SVC$, a parameter $\nu \in (0,1]$ is added in place of parameter C to control the amount of margin errors and support vectors. There is a lower constraint on the fraction of SVs and a maximum limit on the proportion of marginal defects for parameter$n$. (Eq. 1)

$$\min_{\omega,a,\xi,\rho}\left[\frac{1}{2}||x||^2 - \nu\rho + \frac{1}{M}\sum_{j=1}^{M}\xi_j\right]$$

$$subjecttoz_j\left(x.\Phi(w_j) + a\right) \geq \rho - \xi_j, \quad \forall j \in \mathbb{M}$$

$$\xi_j \geq 0, \rho \geq 0 \qquad (1)$$

If variable$\xi_j > 0$then the margin error indicates samples with training mistakes with a condition $(\xi_j > \rho)$ or dwells in the margin if$(\xi_j \in (0,\rho))$, then the marginal among the two classes is$\frac{2\rho}{||x||}$. One way to derive the decision limit is to (Eq. 2):

$$e(w) = sign\left(\sum_{j,i=1}^{M}\lambda_i z_i l(w_j, w_i) + a\right) \qquad (2)$$

Two sets $T_{\pm}$ of the same size$(t > 0)$that contain support vectors w_j about $0 < \lambda_j < 1$ and $z_j = \pm 1$are used to determine the bias term a and marginal factor ρ as shown below (Eq. 3).

$$a = -\frac{1}{2t}\sum_{w,\in T_+,UT_-}\sum_{j=1}^{M}\lambda_i z_j l(w, w_j),$$

$$\rho = \frac{1}{2t}\left(\sum_{w\in T_+}\sum_{j=1}^{M}\lambda_j z_j l(w, w_j) - \sum_{w\in T_-}\sum_{j=1}^{M}\lambda_j z_i l(w, w_j)\right) \quad (3)$$

It should be mentioned that the decision procedure just needs$a$.

3.2. Merchant and Tokenization Module

While the tokenization module managed by the payment gateway is used to generate transaction validation tokens, the seller's module acts as a conduit for financial consumers (the holders of debit and credit cards) to send credit card information. A database with regulated and limited access that is housed on a cloud storage engine is called the token vault. A credit card number is made up of the account number, the check digit, and the bank identity number (BIN), as indicated.

3.3. Card Number Validation

Applying the Luhn formula, the merchant verifies the credit card number. Takinginto consideration that = $\{B_1, B_2, \ldots, B_{m-1}, B_m\}$denotes an n-digit credit card sequence.

The both even and odd products' digits are added up to yield the sums T_1andT_2, respectively, (Eq. 4-6):

$$T_1 = \sum_{l=1}^{m-1} k_l;\ \begin{cases} k_l if k_l < 10 \\ k_l = (k_l/10) + (k_l mod\ 10) if k_l \geq 10 \end{cases} \quad (4)$$

$$T_2 = \sum_{l=2i}^{m-1}(B_l)\forall j = 1, \cdots m-1 \quad (5)$$

$$y = (T_1 + T_2) + B_m \quad (6)$$

The numbers that are in the lth odd and even positions, respectively, are doubled to produce $k_l$and. If y mod 10 = 0, the card value is verified. The credit card value is encrypted using the following cryptographic scheme (Eq. 7 & 8):

$$F(N) \rightarrow d \quad (7)$$

$$C(D) \rightarrow N \quad (8)$$

Encryption, message (plaintext), ciphertext and decryption are represented by the letters $F, N, D$and$C$, in that order.

3.4. Homomorphic

Building up a secure foundation is the essential step in protecting cloud information privacy. Here, cloud data storage security is enhanced by the development of homomorphic-elliptic curve cryptography. The use of mathematical operations on encrypted data is allowed by homomorphic encryption, allowing the decrypted data to have the same matching operations applied to the plaintext data. The process of encoding data so that attackers cannot read it is known as encryption. Two different kinds of encryption methods exist. Figure 2 shows the architectural layout of the proposed system.

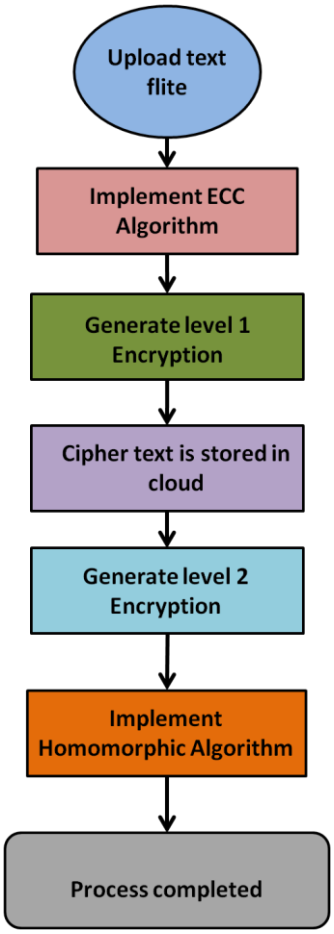


Figure 2: Architectural Layout of the Hybrid Encryption and Decryption Algorithm

Homomorphic and Elliptic Curve Cryptography (ECC). Each slice's data have been encrypted with a different encryption key and cryptographic technique before being uploaded to the cloud. The goal of this method is to cut down on the expense and time associated with storing encrypted information in cloud storage while maintaining a legitimate, safe, and secure data storage method to ward against intrusions and data attacks. The homomorphic algorithm is symmetric key cryptography the data is encrypted and stored using elliptic curve encryption. Several steps of the proposed system are key generation, encryption, and decryption.

Before being saved in the cloud, the data are first encrypted using the keys and the Elliptic Curve algorithm. After that, the cipher text is encrypted another time using the homomorphic algorithm. The public and private keys are generated using the key generation algorithm. When the encrypted data is sent to the user, they utilize their chosen decryption technique to unlock the original text within the encryption.

Key Generation

An algorithm used in public key cryptography is called elliptic curve cryptography. Originally intended simply for use as a digital signature, it was eventually upgraded to include encryption and decryption capabilities. The discrete logarithm underpins the algorithm's strength.

1. Select a prime number B at random.

2. Select two numbers at random, a and d, such that (a<b)and(d<b).
3. Determine c = a ^ dmod b.
4. The public key is C, the private key is D, and both b and a are public.

A public prime number is chosen at random, B. Two further random numbers are selected, one of which is open and the other secret. In this instance, a is the open one and d is the secret. Key creation can be done in different sizes, and as the key gets bigger, so does the security and computational time. This represents a drawback for the millennial generation.

Encryption

Encryption is the process of encoding plaintext or data so that, regardless of the file's visibility, it can be recognized due to its encoding. Even, encryption is a technology employed in data security. A modern encryption method called elliptic curve cryptography encrypts data publicly while decrypting it privately. When compared to other algorithms, it offers security at a lower cost because it provides security through all of the algorithms.

Additionally, it offers secure key transmission between users.

1. $INPUT$: $Datafileandpublickey.$
2. $Encrypteddataistheoutput.$
3. $Createthekeythatispublic.$
4. $Foragivengeneratingfunctionh, Loq = Lov * h.$
5. $Cp = q * histheproducedcipher.$
6. $Usingc = q * Lov + (in * od), thedatafileisencrypted.$
7. $Utilizingthehomomorphicfunction, encryptoncemore.$
8. $Informationiskeptonfileast.$

Then, for the plain text n, select a random integer qt, if the Paillier private key is (oq,ov) and the public key is (M,h). Encryption is the process of (Eq. 9)

$$D = h \text{ ^ } n * qtmodm * m. \qquad (9)$$

It works fit with the cloud's privacy and security of data issues. Data is safely stored in the cloud using elliptic curve and homomorphic curve cryptography. The private key and the input data make up the algorithm's input. Then,$Lov$is formed in the curve public key using the generating function$h$. Similarly, four random numbers qt are used to construct cipher text. Subsequently, the provided input is encrypted using our produced public key and the random algorithm on the cipher text. The encrypted data that is kept in the file is the output.

Decryption

The method of decrypting encrypted text or data allows us to view the original file after it has been decrypted. Following a user request for a data file, the encrypted data undergoes homomorphic processing. After applying elliptic curve cryptography to the cipher text created by the homomorphic process, the entire process may be decrypted using the private key, allowing us to obtain the original data. The process starts with a private key and encrypted data and the result is the original, encrypted file. To create the cipher text, we first need the secret key and the encrypted data. From the curve, we

generate function g by taking the random integer that we obtained using the private key. The process is repeated using the public key for decryption, and the original output is generated by subtracting the output from the cipher text encrypted using the private key. One of the main difficulties with this procedure is that different algorithms create varied key sizes, even when the algorithms are run in an equal manner. To prevent intrusions into the cloud environment, we should authenticate cloud providers. Many techniques exist for this, including authorization and authentication procedures as well as modern cloud security protocols that limit cloud platform access to authorized users exclusively.

1. $INPUT: The encrypted data along with the private key.$
2. $OUTPUT: Initial information.$
3. $The private key is used to decrypt data.$
4. $The private key, d = c * Loq, is used to extract the cipher from encrypted data.$
5. $Value at random from the generating function.$
6. $Cp is equal to Lpr * (qt * h).$
7. $Original data = d + c - Cp.$
8. $Original information is taken out.$

3.5. Tokenization

The encrypted content is stored in the credential vault (token database) along with the token that was created from the credit card number. Using the actual card information, the tokenization function creates tokens after decrypting the encrypted data. An integer sequence is created during tokenization by the use of a random number generator. Tokenization of the real payment card number for every credit card number is represented by the last four numbers on the right, which calculates to the sixth digit from the left position. Since V is the transaction upper bound and $i$is a counter for the number of transactions, let's assume that$j = 1\ to V$.

For the first transaction to produce a token,$j = 1$. (Eq. 10)

$$S_1 = (w.B_l + z) mod B_l\ , \forall m, l = 1 \cdots i, \forall w, z = 0 \cdots 9 \quad (10)$$

For the second transaction, $j = 2$.

Produce a new token S_1 from token S_2 if the credit card number remains the same; else use the card number to generate the tokenS_2.

For the transaction with an upper limit where $j = V$

Token S_V is formed from token$S_V - 1$ if the credit card number stays the same; if not, token S_V is generated from the card number.

A payment card numbers where$j = 1, 2, \ldots$The produced token is$V$, the random single digit numbers w and$z$ are, and the sixth digit is i. The notation mod B_l modifies the expression enclosed in parenthesis by dividing it by B_l and then substituting the resultant value. The random number generator's properties are determined by the parameter wz and the selection of $w$and.

4 Experimental Results

We gather dataset from https://www.kaggle.com/datasets/kartik2112/fraud-detection/data which includes the credit card transaction dataset containing legitimate and fraud transactions. To evaluated the proposed method with existing method such as Encryption (AES), Encoding (BASE64), Hashing (SHA-2) and Tokenization (Agboola et al., 2022).

The web-based solution uses authentication to keep the admin and user sessions apart. During the user session, the user navigates through the confirmation, tokenization, encryption, Luhn test, registration, login, and home page screens. The registration interface is users register and set up their accounts, whereas the home screen displays system information. It takes users to the login screen, where their previously registered passwords and usernames are used to verify their identity. Figure 3 illustrates how to utilize the Luhn Test interface as the initial stage of TE-HC-based encryption and to check if a Master, Verve, or Visa card number is acceptable.

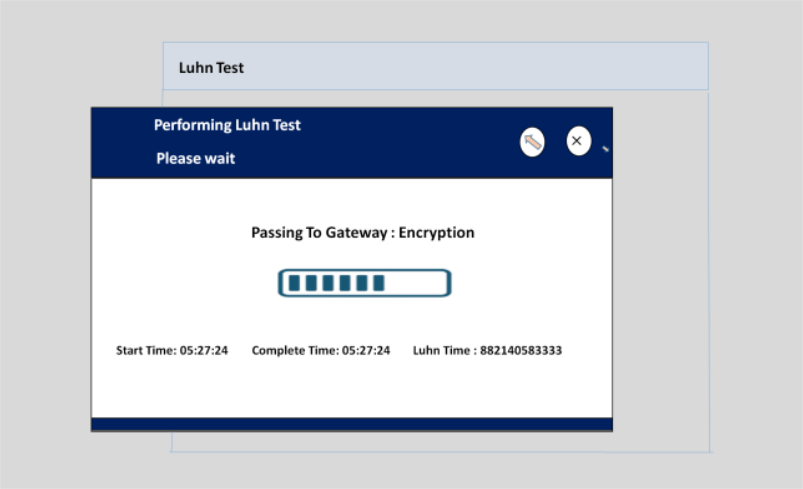
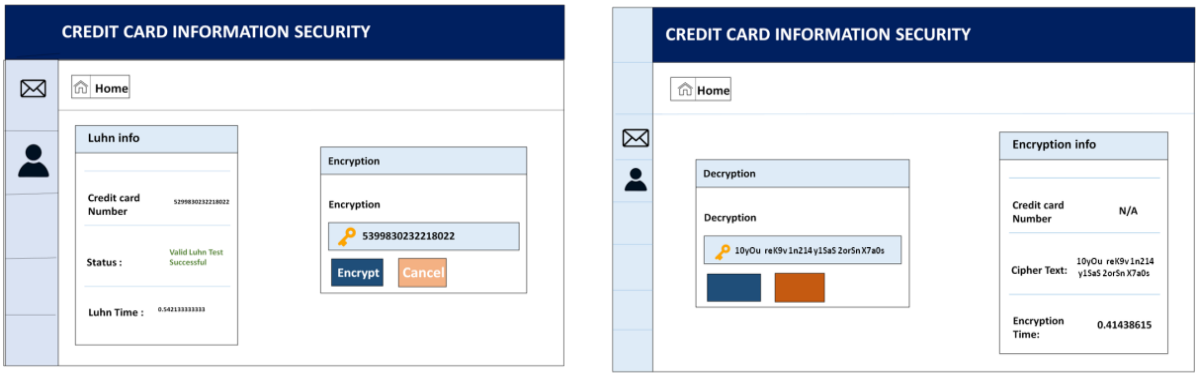


Figure 3: The Luhn Test

The encryption interface, shown in Figure 4(a), which displays the Luhn time, its status, a card number undergoing validation, and an outcome report, signifies the end of this test. As shown in Figure 4(b), the decryption page containing the retrieved ciphertext appears when the encryption interactive procedure is finished. A credit card number cannot be accessed because it is encrypted.



(a) Encryption (b) Decryption

Figure 4: (a) Encryption (b) Decryption Interface

After decryption, the request page depicted in Figure 5 is used to generate a 6-digit token, which is transmitted to the user's pre-registered cell phone number for confirmation and acknowledgment. The system maintains records of user information, including the date and time of the operation, the token that was generated, the token that was received, the acknowledgment times, the new module and the public keys acquired for Elliptic-Homomorphic Cryptography (TE-HC) algorithm-based operations on Master, Verve, or Visa credit card details.

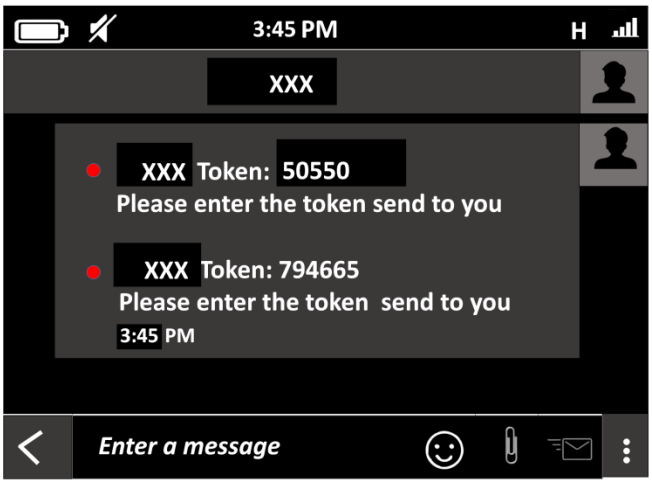


Figure 5: Confirmation Page for Tokens

Table. 1 also displays the users' evaluation of the system using Linkert scale-based evaluation of the system based on the characteristics of speed, security, effectiveness, usability, and user experience.

Table 1: User Evaluation of the System

Index	Speed	Security	Effectiveness	Usability	User Experience
Excellent (5)	540	2280	2000	910 2	1960
Good (4)	1730	800	1680	1360	990
Good (3)	510	20	410	810	250
Average (2)	0	0	0	20	0
Poor (1)	0	0	0	0	0
Mean	5	6	5	5	6

The system's performance was assessed as "very good" overall by the chosen users for "speed," "effectiveness," and "usability." Ratings for "security" and "user experience" were also noted. These scores indicated that the system was well regarded by the chosen users and that they were confident in its ability to securely store information about their credit cards during secure financial transactions.

Memory usage referred to the term used to describe how effectively computer storage resources were allocated and used to process and store encrypted credit card data. Improving memory efficiency guarantees quick data access and cryptographic processes, supporting overall security protocols. Figure 6 and table 2 shows the outcome of memory usage. Compared to existing techniques Advanced Encryption Standard (AES), BASE64, SHA-2, Tokenization our proposed method had lower (TE-HC). In comparison to the existing approach, the suggested method (TE-HC) showed significant improvements in enhancing credit card security data.

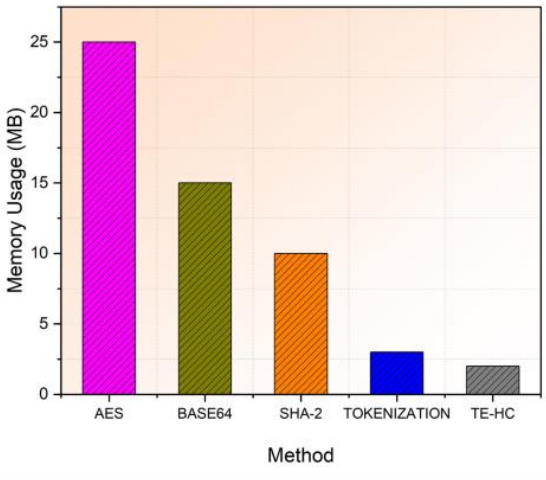


Figure 6: Performance of Memory Usage

Table 2: Analysing in Comparison to Other Models

Method	Memory Usage
AES	25
BASE64	15
SHA-2	10
TOKENIZTION	3
Elliptic-Homomorphic Cryptography (TE-HC)	2

5 Conclusion

In this paper, tokenized Elliptic-Homomorphic Cryptography (TE-HC), an inventive method supported by artificial intelligence (AI) capabilities, is proposed in this study. In addition to enhancing user experience and efficiency, TE-HC also strengthens the integrity of financial information. The system reduces the danger of unwanted access and data exposure by ensuring secured and authorized transmission of credit card details through its merchant and tokenization elements and secure token vault. The results of the implementation show how fast and effective TE-HC is, surpassing conventional techniques in credit card security. TE-HC presents a strong answer to the major problems associated with protecting credit card information in the digital age by combining improved security, effectiveness and user-friendly design. The deployment of TE-HC could be hindered by the requirement for specialist hardware and possible incompatibilities with legacy systems. It offers features including fast transaction processing, hybrid AI-driven intrusion detection and safe tokenization, to improve the security of credit card data.

References

[1] Agboola, R. B., Iro, Z. S., Awwalu, J., & Said, I. N. (2022). Database security framework design using tokenization. *Dutse Journal of Pure and Applied Sciences*, *8*, 16-26. https://doi.org/10.4314/dujopas.v8i1b.3

[2] Alenzi, H. Z., & Aljehane, N. O. (2020). Fraud detection in credit cards using logistic regression. *International Journal of Advanced Computer Science and Applications*, *11*(12). https://doi.org/10.14569/ijacsa.2020.0111265

[3] Campos, R. B. (2024). The Impact of Digitalization on Credit Risk Management in Microfinance Institutions in Nueva Ecija, Philippines. *Indian Journal of Information Sources and Services*, 14(3), 145–156. https://doi.org/10.51983/ijiss-2024.14.3.20

[4] Carrasco, R. S. M., & Sicilia-Urbán, M. Á. (2020). Evaluation of deep neural networks for reduction of credit card fraud alerts. *Ieee Access*, *8*, 186421-186432. https://doi.org/10.1109/ACCESS.2020.3026222

[5] Chakraborty, D., Paul, A., & Kaur, G. (2022). Microeconomics: machine learning model with behavioural intelligence to reduce credit card fraud. *International Journal of Electronic Banking*, *3*(4), 358-378. https://doi.org/10.1504/IJEBANK.2022.128576

[6] Cherif, A., Ammar, H., Kalkatawi, M., Alshehri, S., & Imine, A. (2024). Encoder–decoder graph neural network for credit card fraud detection. *Journal of King Saud University-Computer and Information Sciences*, *36*(3), 102003. https://doi.org/10.1016/j.jksuci.2024.102003

[7] Duan, Y., Zhang, G., Wang, S., Peng, X., Ziqi, W., Mao, J., ... & Wang, K. (2024). Cat-gnn: Enhancing credit card fraud detection via causal temporal graph neural networks. *arXiv preprint arXiv:2402.14708*.

[8] Gamini, P., Yerramsetti, S. T., Darapu, G. D., Pentakoti, V. K., & Raju, V. P. (2021). Detection of credit card fraudulent transactions using boosting algorithms. *Journal of Emerging Technologies and Innovative Research (JETIR)*, *8*(2), 2021.

[9] Habibpour, M., Gharoun, H., Mehdipour, M., Tajally, A., Asgharnezhad, H., Shamsi, A., ... & Nahavandi, S. (2023). Uncertainty-aware credit card fraud detection using deep learning. *Engineering Applications of Artificial Intelligence*, *123*, 106248. https://doi.org/10.1016/j.engappai.2023.106248

[10] Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. *Ieee Access*, *9*, 165286-165294. https://doi.org/10.1109/ACCESS.2021.3134330

[11] Jayanthi, E., Ramesh, T., Kharat, R. S., Veeramanickam, M. R. M., Bharathiraja, N., Venkatesan, R., & Marappan, R. (2023). RETRACTED ARTICLE: Cybersecurity enhancement to detect credit card frauds in health care using new machine learning strategies. *Soft Computing*, *27*(11), 7555-7565. https://doi.org/10.1007/s00500-023-07954-y

[12] Kumar, R. H., Arvind, T., Narayanan, V. B., & Saravanan, P. (2019). Hybrid crypto system using homomorphic encryption and elliptic curve cryptography. *Dr. T. Sethukarasi*.

[13] Kuttiyappan, D., & Rajasekar, V. (2023). AI-enhanced fraud detection: Novel approaches and performance analysis. In *Proceedings of the 1st International Conference on Artificial Intelligence, Communication, IoT, Data Engineering and Security, IACIDS* (pp. 23-25). http://dx.doi.org/10.4108/eai.23-11-2023.2343170

[14] Maurya, S., Shavkidinova, D., Shrivastava, V., & Subrahmanyam, S. (2025). Effects of Green Supply Chain Management Practices on Environmental and Firm Sustainability Performance. *Acta Innovations*, 13-22. https://doi.org/10.62441/actainnovations.vi.401

[15] Noviandy, T. R., Idroes, G. M., Maulana, A., Hardi, I., Ringga, E. S., & Idroes, R. (2023). Credit card fraud detection for contemporary financial management using XGBoost-driven machine learning and data augmentation techniques. *Indatu Journal of Management and Accounting*, *1*(1), 29-35. https://doi.org/10.60084/ijma.v1i1.78

[16] Petrus, J. (2023). A novel approach: Tokenization framework based on sentence structure in indonesian language. *International Journal of Advanced Computer Science and Applications*, *14*(2).

[17] Rabet, F., & Mousavi, S. A. (2017). Performance evaluation of contracting corporations from two dimensions of consumer affairs and financial affairs (Case study: Shiraz municipality). *International Academic Journal of Innovative Research*, 4(1), 14–19.

[18] Rakesh, N., Mohan, B. A., Kumaran, U., Prakash, G. L., Arul, R., & Thirugnanasambandam, K. (2024). Machine Learning-driven Strategies for Customer Retention and Financial

Improvement. *Archives for Technical Sciences*, *2*(31), 269-283. https://doi.org/10.70102/afts.2024.1631.269

[19] Roseline, J. F., Naidu, G. B. S. R., Pandi, V. S., alias Rajasree, S. A., & Mageswari, N. (2022). Autonomous credit card fraud detection using machine learning approach☆. *Computers and Electrical Engineering*, *102*, 108132. https://doi.org/10.1016/j.compeleceng.2022.108132

[20] 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.

[21] Sreeja, S., Suguna, C., Tharani, S., & Rathika, S. K. B. (2018). Digital Security Home. *International Journal of Advances in Engineering and Emerging Technology*, 9(2), 24–27.

[22] Strelcenia, E., & Prakoonwit, S. (2023). Improving classification performance in credit card fraud detection by using new data augmentation. *AI*, *4*(1). https://doi.org/10.3390/ai4010008

[23] Taha, A. A., & Malebary, S. J. (2020). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. *IEEE access*, *8*, 25579-25587. https://doi.org/10.1109/ACCESS.2020.2971354

[24] Uvarajan, K. P. (2024). Integration of artificial intelligence in electronics: Enhancing smart devices and systems. *Progress in Electronics and Communication Engineering*, *1*(1), 7-12. https://doi.org/10.31838/PECE/01.01.02

Authors Biography

Dr. Dipti N. Kashyap is an Assistant Professor in the Department of Mechanical Engineering at Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India. Her research interests include thermal engineering, material science, manufacturing processes, and mechanical system design. She is actively engaged in teaching, mentoring, and conducting research, with publications in reputed journals and presentations at various national and international conferences. Dedicated to fostering innovation and academic excellence, she continues to make valuable contributions to the field of mechanical engineering.

Dr. Kshitij Naikade is an Assistant Professor at Symbiosis Law School, Pune (SLS-P), Symbiosis International (Deemed University) (SIU), Pune, India. His academic expertise spans various areas of law, including constitutional law, legal theory, human rights, and corporate law. Actively involved in teaching, research, and mentoring, Dr. Naikade has published research papers in reputed journals and presented his work at national and international conferences. His dedication to academic excellence and legal scholarship continues to contribute significantly to the field.

Dr. Arvind Kumar Pandey is an Associate Professor in the Department of Computer Science & IT at ARKA JAIN University, Jamshedpur, Jharkhand, India. His research interests include artificial intelligence, machine learning, data mining, cloud computing, and cybersecurity. Actively engaged in teaching, mentoring, and research, Dr. Pandey has published papers in reputed journals, presented at national and international conferences, and contributed to innovative projects in computer science. Committed to academic excellence and technological advancements, he continues to make valuable contributions to his field.

Dr. Nittin Sharma is a researcher at the Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. His research interests encompass interdisciplinary domains, focusing on research impact assessment, innovation management, outcome evaluation, and technological advancements. Actively engaged in research and collaboration, Dr. Sharma has contributed to reputed journals, conferences, and projects aimed at enhancing research quality and societal impact. Dedicated to fostering innovation and academic excellence, he continues to make significant contributions to his field.

Dr. Sadaf Hashmi is an Associate Professor in the Department of ISME at ATLAS Skilltech University, Mumbai, Maharashtra, India. Her research interests include business management, entrepreneurship, skill development, and innovation in education. Actively involved in teaching, mentoring, and research, Dr. Hashmi has published papers in reputed journals, participated in conferences, and contributed to various academic and industry-oriented projects. With a commitment to fostering excellence in management education and interdisciplinary research, she continues to make impactful contributions to her field.

Dr. Sachin S. Pund is an Assistant Professor in the Department of Mechanical Engineering at Ramdeobaba University (RBU), Nagpur, Maharashtra, India. His research interests include thermal engineering, fluid mechanics, advanced manufacturing processes, and automation in mechanical systems. With a strong academic and research background, he has contributed significantly to the field through publications in reputed journals, conference presentations, and collaborative projects. Dr. Pund is dedicated to mentoring students and fostering innovation in mechanical engineering education.