INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

# Secure Transaction of Digital Currency through Fuzzy Based Cryptography

**Vipin Saxena**[1]*, **Pawan Kumar**[1]

**1** Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, Uttar Pradesh, India

OPEN ACCESS

**Received:** 14-06-2023

**Accepted:** 30-08-2023

**Published:** 09-10-2023

**Citation:** Saxena V, Kumar P (2023) Secure Transaction of Digital Currency through Fuzzy Based Cryptography. Indian Journal of Science and Technology 16(37): 3148-3158. https://doi.org/10.17485/IJST/v16i37.1453

* **Corresponding author**.

profvipinsaxena@gmail.com

**Funding:** None

**Competing Interests:** None



Published By Indian Society for Education and Environment (iSee)

**ISSN**
Print: 0974-6846
Electronic: 0974-5645

## Abstract

**Objective:** Internet technology is growing at a very fast rate around the globe and many of the countries are performing currency transaction through online mode. Due to increment of transaction of currency in an exponential manner, there is a need to include proper security features so that hackers or intruders could not hack the digital transaction carrying out between the two parties. **Method:** A new model using Unified Modeling Language (UML) is proposed which is developed in the hybrid mode with a combination of fuzzy rule-based computation, fingerprint authentication, Hash and Elgamal cryptography. The hybrid method is applied for secure transaction of the digital currency. The fuzzy rule based computation is used with Triangular Membership Function (TMF), which is based on current date and time. Fuzzy value creates a secret key and encrypts through Hash algorithm. Elgamal cryptosystem is used for encryption and decryption. The results obtained through hybrid method are tested through the concept of Finite State Machine (FSM) by generating the various test cases. **Findings:** The results obtained through hybrid method are tested through the concept of FSM by generating the various test cases. **Novelty:** In this work, mutual authentication as well as time stamp is also considered and the presented hybrid approach is based upon two-way authentication between client and user which is found to be very effective and may be used by the software industries for the customers especially related to the banking sectors.

**Keywords:** Fuzzy; Hash Algorithm; Cryptosystem; FSM; Test Cases and Validation

## 1 Introduction

The research on the ”cloud computing” is rapidly increasing due to tremendous growth of technology. Cloud computing is based upon the distributed computing approach which is autonomous collection of hand-held devices; well connected through high speed internet facilities. There are various ways for data theft by cyber attacker such that brute force attack, password divination, stealing password, dictionary attack, shoulder surfing and stealing password, etc. To prevent these types of attack, there is need of a better solution for money transaction. The world is moving towards the use of digital currency which is much faster than transfer of manual currency and also it

avoids duplicate transaction of the manual currency. The transfer of the digital currency needs strong security algorithm and from the literature it is observed that many of the traditional algorithms have been breached by the hackers who are accessing the network via high speed internet connectivity. The concept of the hybrid security algorithm shall minimize the said threats, therefore, the present is an attempt in this direction which has three main important components; one is digital currency, second is system model for transfer of currency and third is the fuzzy based biometric authentication through algorithms. Some of the references are available on this concept, but it is observed that the fuzzy based biometric authentication is still missing in the day to day life of the user.

Digital currency was invented by Satoshi Nakamoto in the year 2008 based on the peer to peer technology[(1)]. It was based on the cryptographic electronic money or e-cash invented by cryptographer David Chaum in the year 1983[(2)]. Navamani[(3)] has reviewed the digital currency status around the globe upto 2021. The transfer of the digital currency is based upon the cryptographic trust between the sender and receiver and it does not involve the trust of the third party. But, the security of transfer of digital currency over cloud servers is always concerned as intruders/hackers are watching day to day activities of the users over the network. Swain and Tiwari[(4)] have reported a comprehensive review over the security based on cloud computing and suggested the solution to minimize the risks through a model developed using UML. Kumar and Saxena[(5)] elaborated a hybrid technique for the security of information transmitted from one to another device with high integrity and less time consuming. Two fish, AES, Elgamal and RSA cryptosystem produce the hybrid benefits in terms of computation of speed, encrypted size and use of storage[(6)]. Pittalia[(7)] has compared various types of Hash functions like Whirlpool, Message Digest-5(MD5), Message Digest-4 (MD4), Secure Hash Algorithm-3 (SHA-3), Secure Hash Algorithm-2 (SHA-2) and Secure Hash Algorithm-1 (SHA-1) and obtained the optimized results.

In the present work, fuzzy technique is also used for the security of digital currency. It is true fact that the boolean logic works on 0 or 1 while fuzzy logic does not work completely on 0 or 1 but lies between 0 and 1. The fuzzy function works on input and set of rules and complete fuzzy system has six attributes like input, fuzzifier, inference engine, defuzzifier, fuzzy knowledge base and output. The fuzzy logic gives flexibility for solving the research problem by considering all the parameters involved in the problem and obviously provides better solution in comparison of the normal sets of parameters. It touches humanity to take more accurate decision that is the reason; it is widely used in the Artificial Intelligence and Machine Learning. From the literature, it is revealed that there is some research work available on the fuzzy theory applied over the security system. Valdes-Ramirez et al.[(8)] have looked at the most popular fingerprint feature representations and noted the trends of various representations for verification of the individual identity. Hindi et al.[(9)] have discussed the techniques for extracting the image features like Reduced Centre Symmetric Local Binary Pattern (RCSLBP) method and C-clustering and further compared the effectiveness and fixed the features when the fingerprint is rotated. Mohan and Kavithadevi[(10)] have developed Elgamal cryptosystem alongwith Decisional Diffie-Hellman. The contents are to be encrypted after broking it into equal-sized of chunks, and each one has chunk address and the complete system is probabilistic because of chunk scanning. Azam et al.[(11)] have studied on creating the triangular membership function's parametric values. The Gaussian membership function's parameters are first generated using the Fuzzy C-means approach and the numbers are used to compute an approximation of the triangular membership function's parameters using a series of equations. The quality of web services data is also applied to the suggested technique. Bian et al.[(12)] have implemented the Bio-AKA algorithm which provides strength of fingerprint and physically unclonable function. The system suggested that can guarantee to the users in terms of privacy without requiring a password and enable the mutual authentication via a key agreement. In the year 2021, Irshad et al.[(13)] have implemented fuzzy extractor-based methods in the loop and the two-factor fingerprint identification technique which enables the effective and safe integration of physically unclonable functions.

Before solving the research problem, a system model must be proposed through any modelling language. Unified Modeling Language is backbone of all modelling languages as the model can be easily developed through any object oriented programming language. After evolution of the Python programming language, UML is widely used in the software industries for making the blue print of the software problem. Hence, in the present work and before defining the research problem, a UML system model is developed for the fuzzy based authentication based on the Elgamal technique for transferring of the digital currency. For the validation purpose, the UML system model is converted into FSM which has five tuples {Q, Σ, q, F, $\delta$}, where, Q, Σ, q, F, $\delta$ represent set of all states, set of all inputs, initial state of machine, set of final states and transition function, respectively. In the software industries, many of the digital systems are controlled by the concepts of FSM, therefore if the FSM has flaws, the security of the entire system might be at risk. Xiao et al.[(14)] have developed FSM model and implemented through Hyper Sensor Markup Language (HSML) with composite architecture of Internet of Things (IoT). Wijayanti[(15)] also developed a model for Jungle Adventure Game for the survival skills.

In the year 2019, Gope et al.[(16)] have implemented security for wireless senser network which combined lightweight cryptographic, Hash cryptographic, XOR logic operation and physically unclonable function. Maitra et al.[(17)] have implemented

security for cloud-based Internet of Things (IoT) devices which applied Elgamal cryptography, user login with the help of password and fingerprint authentication. In the year 2020, Kumar et al. [18] have implemented that iris pattern is encrypted by Elgamal cryptography and blockchain-based smart contract can help to ensure the integrity of the patterns and the accuracy of the matching process. Bao and You [19] have suggested identity identification method that combines blockchain with fuzzy extractor technology. The user credential information stored in blockchain and fuzzy extractor provided security for fingerprint. In the year 2022, Wahaballa [20] has implemented security for IoT device-based payment system. Security for payment through IoT device, used two lightweight cryptography and identity-based signature.

From the above review of work, it is observed that the hybrid approach based on the fuzzy rule-based computation, fingerprint authentication, Hash and Elgamal cryptography is never touched by the researchers, hence, hybrid method based on these aspects is applied for secure transaction of the digital currency. The important part of this approach is that the approach is based upon real date and time. Secret key is generated through fuzzy concept and further encrypted through Hash algorithm and thereafter Elgamal cryptosystem is used for encryption and decryption. The computed results are validated through FSM by generating the various test cases. The important part of the proposed work is that the hybrid approach is based upon mutual authentication as well as time stamp for secure transaction of the digital currency.

## 2 Methodology

The proposed model works on current date and time of transactions, and it provides a key based on current time stamp and date. With the help of key system, it provides mutual authentication between client and server nodes. User ID and Password are encrypted by Elgamal cryptography and needs to enter account page for withdrawing money which needs fingerprint authentication and further unique key is based on current date and time using fuzzy concept.

Due to evolution of digital era, transactions in digital form are increasing day by day in exponential manner. But hackers are attempting to steal the digital currency across the network, therefore, it is necessary to propose a UML system model as shown in the Figure 1 to enhance the security level by incorporating the fuzzy rule-based encryption and decryption. Let us describe some key benefits to select the UML, as it is most popular modelling language among the software developers. It creates unified software design which can be easily coded by the software coder through any object-oriented programming language. It supports three aspects, one is structural modelling, second is dynamic modelling and third one is the functional modelling. Structural modelling produces blue print of the software problem while dynamic shows how it works at the run time and lastly functional modelling represents the movement of the data from one module to another module. Let us discuss the designed system model in UML which is represented in the following diagram, customer has multiple accounts from multiple banks. Customer enters UID and Password on login page which is provided by bank. The bank's server authenticates to the Customer through UID and Password. Customer's UID and Password are encrypted and decrypted by the class El_gamal_cryptography. The class Fuzzy_compu_Hash, computes Fuzzy_Value based on current day, month, year, hour, and minute. Then Fuzzy_Value is encrypted by hash and has a class Transaction for input the amount. If Customer enters amount properly then the class Fingerprint_Scanner scans the fingerprint of the Customer.

In the above diagram, many customers including the staff of the bank must have the high speed internet facilities to access the data stored over the cloud servers which has all the records entered by the bank. The relationship in the model is many to many which depicts that many customers are having multiple/single account in a single or multiple banks. Authentic identity and password are to be set by the user by opening the bank page. When Customer enters user id (UID) and Password, then fuzzy computation is performed at end of the user in which current date and time are shared and transferred over the cloud through the following algorithm [19]:

elgamal_algo(m←message)
key_generation()
Pr←Large_prime_number where Pr∈ group G=<Z*pr, A>
selectprivate_key →A such that 1 ≤A ≤ Pr -1
select generator g→primitive root in G= <Z*pr, A>
$B=g^A \text{mod} Pr$
Public_key← (g,B,Pr)
Private_key←A
encryption()
select random integer r → in G= <Z*pr, A> such that 1 ≤r≤ Pr -1
$C_{1\leftarrow} g^r \text{mod} Pr$
$C_{2\leftarrow} (m.B^r) \text{ mod } Pr$
decryption()

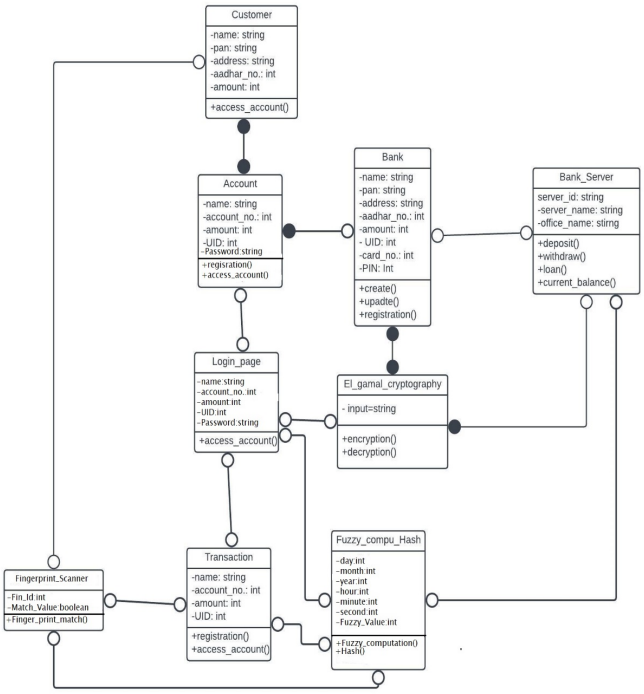


**Fig 1.** UML Class Model

$m \leftarrow ( C_2(C_1{}^A)^{-1} \bmod Pr$

The above algorithm is a public key cryptosystem which has three parts namely key generation, encryption and decryption. It is based upon the asymmetric key distribution between the parties. It follows the rule of cyclic group and complicated keys can be generated through discrete logarithmic. In the above, the variable m represents as message to be encrypted and decrypted using generated keys as above, A is private key while B is public key. The primitive root is computed in the cyclic group G<Z*pr, A>. Further, fuzzy computation based on current date and time through Triangular Membership Function (TMF) is proposed which works on input and set of rules. The input is current time and date, set of rules are defined based on time and date.

Fuzzy_computation(day, month, year, hour, minute)

Fuzzifier← linguistic variables

day, month, year, hour, minute ← current date and time

rules← define set of rules

In the above, fuzzy value computes the current date, time and some set of rules which may be applied server and user sides. If the value at server and user side is same then it will authenticate for transaction of digital currency otherwise transaction will be failed. The reason for selection of the fuzzy logic is that it is widely used in the commercial as well as for practical purpose. The fuzzy based algorithms can be easily coded through object-oriented programming language. In the present work, fuzzy computation combines the following definitions:

**A. Input variables**

There are number of input variables which play role for taking the decision about the Fuzzy_computation(). There are five input variables namely year, date, month, hour and minute and all variables are defined as membership function like dismal, poor, mediocre, average, decent, good and excellent.

**B. Output variables**

The output variable of Fuzzy_computation() is Fuzzy_Value which may be extended low (el), very low (vl), low (l), medium (m),high (h), very high (vh) and extended high (eh).

**C. Fuzzy rules**

Fuzzy rules make fuzzy relationship between the input and output variables. The set of rules are considered as given below:

R1→ If date is dismal and month is dismal and year is dismal and hours is dismal and minute is dismal then Fuzzy_Value is el.

R2→ If date is poor and month is poor and year is poor and hours is poor and minute is poor then Fuzzy_Value is eh.

R3→ If date is mediocre and month is mediocre and year is mediocre and hours is mediocre and minute is mediocre then Fuzzy_Value is vh.

R4→ If date is average and month is average and year is average and hours is poor and minute is mediocre then Fuzzy_Value is h.

R5→ If date is decent and month is decent and year is decent and hours is dismal and minute is dismal then Fuzzy_Value is m.

R6→ If date is good and month is good and year is good and hours is average and minute is average then Fuzzy_Value is l.

R7→ If date is excellent and month is excellent and year is excellent and hours is good and minute is good then Fuzzy_Value is vl.

R8 → If date is mediocre and month is average and year is poor and hours is decent and minute is average then Fuzzy_Value is el.

R9→ If date is dismal and month is decent and year is dismal and hours is excellent and minute is decent then Fuzzy_Value is vl.

R10 → If date is excellent and month is average and year is dismal and hours is excellent and minute is excellent then Fuzzy_Value is eh.

The proposed method is a combination of Fuzzy_computation(), elgamal_algo(message) and Finger_print_match() and the reason for selection of hash value is that it is unique value and handles large amount of data used for transactions over the communication channel; and it is proposed below:

```
Fuzzy_rule_based_currency_transaction(UID, Password, Fuzzy_Value)
#At User Login Page
U ←UID
P← Password
EncrU←Encrypt(U)
EncrP←Encrypt(P)
FV_user_end←Fuzzy_computation(day, month, year, hour, minute)
Hash_user_end←FV_user_end
# At Server Side
DecrU←Decryption(EncrU)
DecrP←Decryption(EncrP)
FV_server_side ←Fuzzy_computation(day, month, year, hour, minute)
Hash_user_end←FV_server_side
IF (U == X && P ==Y) && (Hash_user_end==Hash_server_side)
Shows_customer_info( )
Withdraw_transaction ←select
amount ← enter Amount
IF available_amount<amount
Scan_fingerprint← fingerprint
FV_user_end←fuzzy rule-based computation
Hash_user_end←FV_user_end
#At the server side
FV_server_sideFuzzy_computation(day, month, year, hour, minute)
Hash_user_end←FV_server_side
IF (Scan_fingerprint == True) &&(Hash_user_end==Hash_srever_side)
Transaction_successful()
ELSE
Transaction_failed()
ELSE
Transaction_failed()
ELSE
Transaction_failed()
```

The above model has two phases; in the first phase user authentication is to be completed. The Customer requests to server by entering the UID and Password credentials. When Customer's request is seen by the administrator, then fuzzy rule-based

computation will be occurred. If UID and Password both are valid then system will authenticate to the Customer. In the second phase, when Customer desires to finish the Transaction then further it needs fingerprint authentication and at the same time fuzzy rule-based computation will be occurred. If matched then Transaction will be successful otherwise failed. Further, for validation purpose, the UML class diagram as shown in the Figure 1 is converted into FSM in which each state represents class depicted in the UML diagram and each event represents relationship between classes. List of states and events are given in the Tables 1 and 2, respectively.

**Table 1.** List of State

| Name of State | Description |
|---|---|
| $q_0$ | Customer |
| $q_1$ | Account |
| $q_2$ | Bank |
| $q_3$ | Bank_Server |
| $q_4$ | Login_Page |
| $q_5$ | Elgamal_cryptography |
| $q_6$ | Fingerprint_Scanner |
| $q_7$ | Fuzzy_comput_Hash |
| $q_8$ | Transaction |

Relationship between two classes is represented by the event in the UML class diagram and the description of events is given below in the Table 2.

**Table 2.** List of Event

| Name of Event | Description |
|---|---|
| A | Customer accesses account |
| B | Account's information sends to Bank server |
| C | Customer's account information transferred by Bank |
| D | Bank sends Customer's information to Bank server |
| E | Bank server transfers account information to bank |
| F | Reply to Customer |
| G | Customer enters UID and Password |
| H | Sends Customer's account information |
| I | Transfer UID and Password for encryption by Elgamal |
| J | Encrypted UID, Password and Hash value of Fuzzy computation send to Bank server |
| K | Request for Hash value of Fuzzy computation |
| L | Transfer of Hash value of Fuzzy computation |
| M | Fingerprint scan |
| N | If Fingerprint and Hash value of Fuzzy computation are matched |
| O | Enter proper amount for currency transaction |
| P | If not enter proper amount |
| Q | If Fingerprint and Hash value of Fuzzy computation are not matched |

On the basis of above, a FSM diagram is designed and represented below in the following Figure 2.

The Figure 2 represents the transaction of digital currency based on fuzzy rule, fingerprint authentication and Elgamal cryptography. The states $q_0$ and $q_4$ represent Customer and login page, respectively. The events g and f represent relationship between two states, the event g represents Customer enters UID and Password and the event f represents Reply to Customer. In the similar fashion, the above diagram is designed.

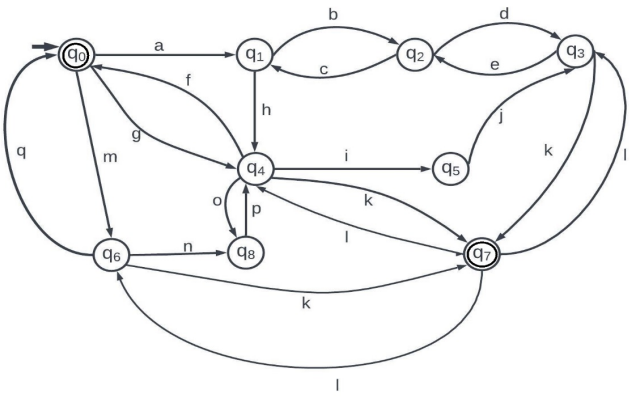


**Fig 2.** FSM for Authentication and Validation

## 3 Results and Discussion

For validating the proposed model, a concept of FSM is used and the various test cases have been designed using important parameters for enhancement of the security level. The reason for selection of FSM technique is that it can visualize the system very well and how the system is working, hence it is very useful for validating the system model. In this case, there are three most important parameters of test cases, first is UID, Password and value of fuzzy computation, second is fingerprint and value of fuzzy computation, third is entry of proper amount which must not greater than available amount in the account of Customer. On the basis of various selected parameters, the following test cases are designed:

Test Case1: Invalid UID, Password and Fuzzy_Value

From UID, Password and Fuzzy_Value, if one of parameter is not matching then server will send an error message to the customer as depicted below (Figure 3):

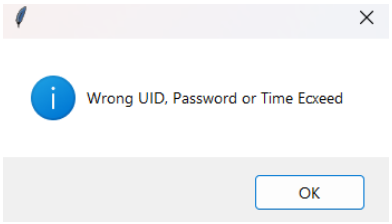


**Fig 3.** Representation of Invalid login Window

Test case 2**:** Fingerprint and Fuzzy_Value

The bank server verified the customer fingerprint and value of fuzzy computation, if it will not match then it will send error message to customer as depicted below (Figure 4):

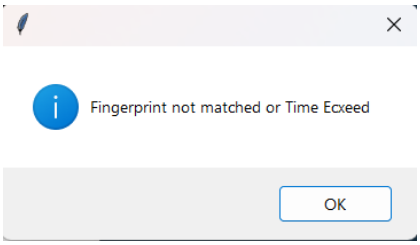


**Fig 4.** Representation of Fingerprint Authentication

Test case 3: Enter proper amount

If the customer does not enter proper amount, then the bank server will send a message to the Customer. Proper amount means→enter withdrawn amount may not greater than available amount (Figure 5).

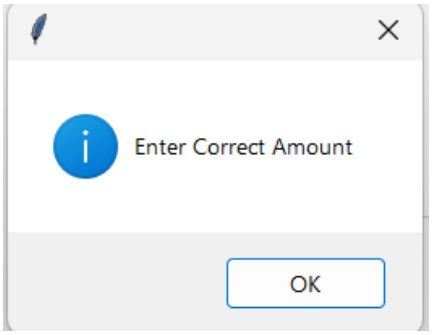


**Fig 5.** Representation of Invalid Amount Window

Digital transaction over the network has high risk which must need the high level security. In the proposed method, a concept of asymmetric key exchange algorithm, hash function, fuzzy computation, and fingerprint is applied. Asymmetric key exchange algorithm is considered as Elgamal, Hash, and fuzzy computation is done through triangular membership function. When Customer logins with valid UID and Password then information is transferred to the server with key, which is generated by Elgamal algorithm, along with fuzzy value computation based on current time which is encrypted by Hash function. Server receives request, decrypts the data and computes Fuzzy_Value and further encrypts by Hash function at the server side. If UID and Password are matched with database and Hash value at server and user side are same then request is accepted otherwise it is rejected. Fuzzy computation is defined based on current time and date. The variables defined are hour, minute, date, month and year. The resultant of all rules is depicted below in the Figure 6.

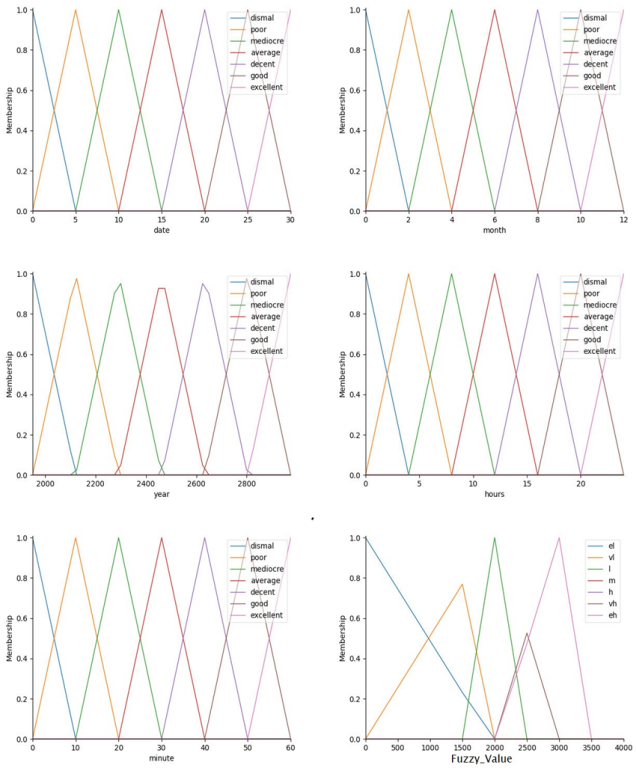


**Fig 6.** Traingular Representation of Fuzzy Rules

All fuzzy variables are defined as: dismal, poor, mediocre, average, decent, good, excellent. Fuzzy rules are defined by IF THEN and fuzzy computation based on current day, month, year, hour, minute and set of rules is represented by Figure 7.

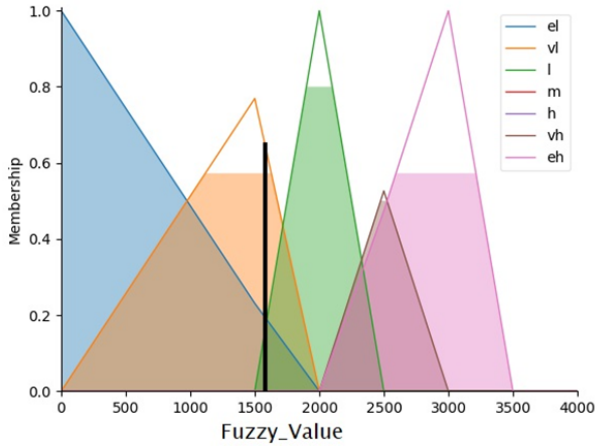


**Fig 7.** Fuzzy Computation based on Input and Set of Rules

Triangular membership function for fuzzy computation is used with input variables, fuzzy sets, and set of rules and further resultant which computes the Fuzzy_Valueis sent along with encrypted data to the bank's server, then server decrypts the data. The Fuzzy_Value is computed at the server side at the time of login, if Fuzzy_Value of sender and server are same then request is accepted and sends signal for next step to the user. When user withdraws money then system requests to scan fingerprint, at this time Fuzzy_Value is again computed. Fingerprint and Hash value of fuzzy are computed and sent to the server. The server again computes the fuzzy computation and encrypts with Hash value. If fingerprint matched with database and Hash value are same from both the sides then transaction is successful otherwise it is failed. In the present approach, all the factors like real time computation, Hash cryptography, asymmetric cryptography, two factor authentication, finger print authentication, mutual authentication, session key agreement and fuzzy system are considered while from the literature, it is found that all these aspects in one research paper are not considered, therefore, a comparison Table 3 is given below which is based upon the latest research work related to present work.

**Table 3.** Comparison of Various Approaches with Proposed Method

| Method | (12) | (13) | (16) | (17) | (18) | (19) | (20) | Present |
|---|---|---|---|---|---|---|---|---|
| **Real Time Computation** | No | No | No | No | No | No | No | Yes |
| **Hash Cryptography** | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| **Asymmetric Cryptography** | No | No | No | Yes | Yes | Yes | Yes | Yes |
| **Two Factor Authentication** | Yes | Yes | Yes | No | No | Yes | No | Yes |
| **Fingerprint Authentication** | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| **Mutual Authentication** | Yes | Yes | Yes | Yes | No | No | Yes | Yes |
| **Session Key Agreement** | Yes | Yes | Yes | Yes | No | No | Yes | Yes |
| **Fuzzy System** | Yes | Yes | No | No | No | Yes | No | Yes |

On the basis of Table 3, the computation cost is also computed which is given in the Table 4.

The above table represents comparison among the computational cost of algorithms available in the literature and proposed algorithm which is taking computational cost of $4T_h$ while Elgamal cryptography, biometric authentication operation and fuzzy logic control operation have taken computational cost as $2T_{ECG}$, $2T_{BA}$ and $2T_{BA}$, respectively. In the present method, the total computational cost is $4T_h + 2T_{BA} + 2T_{ECG}$ and it has less than the other algorithms except algorithm [19]. Due to some complex computational methods which are used in other algorithms like $T_{PUF}$, $T_{FEG}$ and $T_{FEC}$, take more time than proposed algorithm.

**Table 4.** Comparison of the Computational Cost with Existing Algorithm

| Schemes | Registration | Client Side | Server Side | Total Cost |
|---|---|---|---|---|
| (12) | $7T_h + 1T_{PUF} + 1T_{FEG}$ | $12T_h + 1T_{PUF} + 1T_{FEG} + 1T_{FEC}$ | $7T_h + 1T_{FEC}$ | $26T_h + 2T_{PUF} + 2T_{FEG} + 2T_{FEC}$ |
| (13) | $8T_h + 1T_{PUF} + 1T_{FEG}$ | $16Th + 1T_{PUF} + 1T_S + 1T_{FEG} + 1T_{FEC}$ | $7T_h + 1T_{FEC} + 3T_S$ | $31T_h + 2T_{PUF} + 4T_S + 2T_{FEG} + 2T_{FEC}$ |
| (16) | $2T_h + 1T_{PUF} + 1T_{FEG}$ | $10T_h + 5T_{PUF} + 1T_{FEC}$ | $7T_h$ | $21T_h + 6T_{PUF} + 1T_{FEG} + 1T_{FEC}$ |
| (17) | - | $2T_{EXP} + 5T_h + T_{MUL}$ | $T_{EXP} + 7T_h + T_{MUL}$ | $3T_{EXP} + 12\ T_h + 2T_{MUL}$ |
| (18) | $1\ T_h + 1\ T_{ECG} + 1T_{IGEN()}$ | $1\ Th + 1\ T_{ECG} + 1T_{IGEN()}$ | $1Th + 1T_{ECG} + 1T_{IGEN()}$ | $3Th + 3\ T_{ECG} + 3T_{IGEN()}$ |
| (19) | $1T_h + 1T_{FEG} + 1T_{MTC}$ | $1T_h + 1T_{FEG} + 1T_{MTC}$ | $1T_h + 1T_{FEG} + 1T_{MTC}$ | $3T_h + 3T_{FEG} + 3T_{MTC}$ |
| (20) | $2T_h + 1T_{FEG} + 1\ T_{SIG}$ | $2T_h + 1T_{FEG} + +1\ T_{SIG}$ | $2T_h + 1T_{FEG} + +1\ T_{SIG}$ | $6T_h + 3T_{FEG} + 3\ T_{SIG}$ |
| **Proposed Method** | - | $2T_h + 1\ T_{ECG} + 1T_{BA} + 2\ T_{FLC}$ | $2T_h + 1T_{ECG} + 2T_{FLC} + 1T_{BA}$ | $4T_h + 2T_{ECG} + 2T_{BA} + 4T_{FLC}$ |

$T_h$ = Hash computation, $T_{PUF}$ = Physical Unclonable Function, $T_{FEG}$ = Fuzzy Extractor Generation, $T_{FEC}$ = Fuzzy Extractor Reproduction, $T_S$ = Symmetric Cryptography, $T_M$ = Modular Computation, $T_{MTC}$ = Merkel Tree Algorithm, $T_{ECG}$ = Elgamal Cryptography, $T_{SIG}$ = Signature, $T_{FLC}$ = Fuzzy Logic control, $T_{BA}$ = Biometric Authentication, $T_{IGEN()}$ = Iris Code Generation and Compression, $T_{EXP}$ = Exponential operation, $T_{MUL}$ = Multiplication operation.

## 4 Conclusion

From the above work it is concluded that is a versatile modelling language which can be used to propose the system model and the model can be easily converted into any object-oriented programming language and even system model can be easily used to convert into FSM which can lead to generation of the various test cases. In the hybridization of various techniques, combinations of time, date, fuzzy computation, fingerprint authentication, Hash and Elgamal cryptography have been applied and if any one of above combinations are not matched then transaction will have failed which will definitely minimize the crimes happening to steal the digital currency. Fuzzy computation generates a secret key based on current day, month, year, hour and minute further fuzzy value is encrypted by Hash cryptography. If hacker has an idea about the current time and date then it needs the set of rules which are very difficult to crack either at user or server side. The proposed biometric authentication consists of real time computation, Hash cryptography, asymmetric cryptography, two factor authentications, fingerprint authentication, mutual authentication, session key agreement and fuzzy system which never studied before, and software industries may use the proposed work for securing the transfer of digital currency however the work can be extended using the concept of artificial intelligence and machine learning. On the above aspects, the other conventional cryptographic algorithms can be combined to form new hybrid algorithms which will increase the efficiency in terms of secure transaction of the digital currency over the communication channel.

## References


1) Nakamoto S. Bitcoin: A Peer-To-Peer Electronic Cash System, Decentralized Business Review. 2008. Available from: https://assets.pubpub.org/d8wct41f/31611263538139.pdf.
2) Cryptocurrency. 2023. Available from: https://en.wikipedia.org/wiki/Cryptocurrency#.
3) Navamani TM. A Review on Cryptocurrencies Security. *Journal of Applied Security Research*. 2023;18(1):49–69. Available from: https://doi.org/10.1080/19361610.2021.1933322.
4) Swain S, Tiwari RK. Cloud Security Research- A Comprehensive survey. *International Journal of Electronics Engineering and Applications*. 2020;8(2):29–39. Available from: https://doi.org/10.30696/IJEEA.VIII.II.2020.29.39.
5) Kumar J, Saxena V. Hybridization of Cryptography for Security of Cloud Data. *International Journal of Future Generation Communication and Networking*. 2020;13(4):4007–4014. Available from: http://sersc.org/journals/index.php/IJFGCN/article/view/34754/19261.
6) Jintcharadze E, Iavich M. Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. *2020 IEEE East-West Design & Test Symposium (EWDTS)*. 2020;p. 1–5. Available from: https://doi.org/10.1109/EWDTS50664.2020.9224901.
7) Pittalia PP. A Comparative Study of Hash Algorithms in Cryptography. *International Journal of Computer Science and Mobile Computing*. 2019;8(6):147–152. Available from: https://www.academia.edu/download/59869343/V8I6201928.pdf.
8) Valdes-Ramirez D, Medina-Perez MA, Monroy R, Loyola-Gonzalez O, Rodriguez J, Morales A, et al. A Review of Fingerprint Feature Representations and Their Applications for Latent Fingerprint Identification: Trends and Evaluation. *IEEE Access*. 2019;7(1):48484–48499. Available from: https://doi.org/10.1109/ACCESS.2019.2909497.
9) Hindi A, Dwairi MO, Alqadi Z. Analysis of Procedures Used to Build an Optimal Fingerprint Recognition System. *International Journal of Computer Science and Mobile Computing*. 2020;9(2):21–37. Available from: https://ijcsmc.com/docs/papers/February2020/V9I2202008.pdf.

10) Mohan M, Kavithadevi MK, V JP. Improved ElGamal Cryptosystem for Secure Data Transfer in IoT Networks. *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. 2020;p. 295–302. Available from: https://doi.org/10.1109/I-SMAC49090.2020.9243407.
11) Azam MH, Hasan MH, Hassan S, Abdulkadir SJ. Fuzzy Type-1 Triangular Membership Function Approximation Using Fuzzy C-Means. *2020 International Conference on Computational Intelligence (ICCI)*. 2020;p. 115–120. Available from: https://doi.org/10.1109/ICCI51257.2020.9247773.
12) Bian W, Gope P, Cheng Y, Li Q. Bio-AKA: An efficient fingerprint based two factor user authentication and key agreement scheme. *Future Generation Computer Systems*. 2020;109:45–55. Available from: https://doi.org/10.1016/j.future.2020.03.034.
13) Irshad A, Usman M, Chaudhry SA, Bashir AK, Jolfaei A, Srivastava G. Fuzzy-in-the-Loop-Driven Low-Cost and Secure Biometric User Access to Server. *IEEE Transactions on Reliability*. 2021;70(3):1014–1025. Available from: https://doi.org/10.1109/tr.2020.3021794.
14) Xiao R, Wu Z, Wang D. A Finite-State-Machine model driven service composition architecture for internet of things rapid prototyping. *Future Generation Computer Systems*. 2019;99:473–488. Available from: https://doi.org/10.1016/j.future.2019.04.050.
15) Andrea R, Wijayanti S, Nursobah. Finite State Machine Model in Jungle Adventure Game an Introduction to Survival Skills. *International Journal of Information Engineering and Electronic Business*. 2021;13(4):55–61. Available from: https://doi.org/10.5815/ijieeb.2021.04.05.
16) Gope P, Das AK, Kumar N, Cheng Y. Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks. *IEEE Transactions on Industrial Informatics*. 2019;15(9):4957–4968. Available from: https://doi.org/10.1109/TII.2019.2895030.
17) Maitra T, Obaidat MS, Giri D, Dutta S, Dahal K. ElGamal cryptosystem-based secure authentication system for cloud-based IoT applications. *IET Networks*. 2019;8(5):289–298. Available from: https://doi.org/10.1049/iet-net.2019.0004.
18) Kumar MM, Prasad MMV, Raju USN. BMIAE: Blockchain-Based Multi-Instance IRIS Authentication Using Additive Elgamal Homomorphic Encryption. *IET Biometrics*. 2020;9(4):165–177. Available from: https://doi.org/10.1049/iet-bmt.2019.0169.
19) Bao D, You L. Two-factor identity authentication scheme based on blockchain and fuzzy extractor. *Soft Computing*. 2023;27(2):1091–1103. Available from: https://doi.org/10.1007/s00500-021-05936-6.
20) Wahaballa A. Lightweight and Secure IoT-Based Payment Protocols from an Identity-Based Signature Scheme. *Electronics*. 2022;11(21):3445. Available from: https://doi.org/10.3390/electronics11213445.