Accountancy Business and the Public Interest
ISSN: 1745-7718

Volume: 40
Issue Number:12

CREATE SECURE ONLINE TRANSACTIONS USING A RICH-RELIABILITY ALPHANUMERIC CODE PROCEDURE USING TWO-STEP AUTHENTICATION TECHNIQUES

D.SARAVANAN[1], Dr. ANUSHA SREERAM[2], Dr. DENNIS JOSEPH[3],
Dr. KVSSN MURTY[4] and Dr. SIVA G.V[5]

[1,2,3,4,5] Faculty of Operations & IT, ICFAI Business School (IBS), Hyderabad, The ICFAI Foundation for Higher Education (IFHE), (Deemed to be university u/s 3 of the UGC Act 1956), Hyderabad-India.

Abstract

Today, getting products online is one of the easiest and most convenient options for users. Plenty of service providers across the globe offer this service, allowing users to order any product from any geographical location. Users can select, view, and compare products online, either with an account or without one. Once a user selects a product, it is necessary to pay for it using one of the available payment mechanisms. Most payment gateways today are enabled with two-way authentication mechanisms. Each time a user enters their credentials, a random Rich Reliability Alphanumeric Code (RRAC) is generated and communicated to the user via a short text message. This information is generated randomly, so even if the same user continues the operation or initiates another transaction, they will never receive the same RRAC. This process is performed by the RRAC server using symmetric key authentication mechanisms. This information exchange is highly secure because the key is known only to the transaction creator and receiver. Any hacker attempting to steal the RRAC would have no clue as to which product the information pertains to. In our proposed paper, this process is explained in a three-step mechanism: RRAC recordkeeping, RRAC sign-on, and RRAC process. The proposed mechanism is more secure than the existing one-time password mechanism. Our investigation outcomes have proved that this method is more secure and efficient.

Rich Reliability Alphanumeric creation

I. INTRODUCTION

Today, users have the flexibility to pay for any function using net-based transactions, which can be done via net banking, UPI, and card-based transactions. With every purchase, users are required to pay the amount via a link or a site that prompts them to use the payment gateway. However, this process increases the chance of users misleading credit providers. Figures 1–3 below clearly illustrate how this type of transaction has increased globally over time. The amount involved in these scams has increased due to various factors, one of which is security concerns associated with card transactions.

Nowadays, most card systems are enabled with two-factor authentication. From the user's side, they are asked to enter a four-digit secret code. However, this code can be easily tracked or recorded by hackers. Many users are unaware of the importance of the four-digit secret code and trust others, often sharing this number. Additionally, they may not change this number for many years. Most of these numbers can be easily predicted by hackers, such as using birth dates, school or college completion years, or relatives' birth dates. This type of information is easily predictable and crack able by hackers.

The second step of authentication is provided by the service provider. Normally, the service provider also provides a four-digit authentication code after the request is made from the sender's side. Once the first step of verification is completed, users are required to enter the service provider's authentication code. This code is generated randomly by the service provider each time a transaction is initiated by the user. Even if the same user performs multiple transactions on the same day, the generated code is different each time. This code is communicated to the sender via SMS or email. Users are required to enter this number to complete the transaction.

This random number generation provides strong protection from the user's side, as it is not easy for hackers to guess and does not provide any clues. Each time this Rich Reliability Creation Text (RRAC) is generated by the provider, it is done with the help of three different servers. One server initially collects the user's credentials and is responsible for registering the user as a customer after proper verification by the user. The second server allows the user to enter the system using the credentials generated in step one, verifying the secret code provided to the user at the time of registration and allowing the user to continue their operations. The third server is responsible for generating the Rich Reliability Creation Text whenever the user completes the first step of authentication. This number or text is generated randomly for each of the user's transactions.

There are several ways in which these details are stolen from the user. Most often, this information is taken when a user makes a purchase, with someone standing nearby to watch the credentials entered by the user. In many cases, users receive random calls asking for their credentials. This process is illustrated in Figure 4. Additionally, users often receive fake calls in the name of service providers requesting their details. Another common method of information collection is through garbage.

Many customers throw their credit card bills or transaction receipts into the trash without properly tearing them, which can allow hackers to easily collect details. Sometimes, users forget to collect their bills or refresh the process while shopping, which enables hackers to collect customer credentials. This type of information is typically stored in sellers' databases, and hackers may pay certain amounts to sellers to obtain these details.

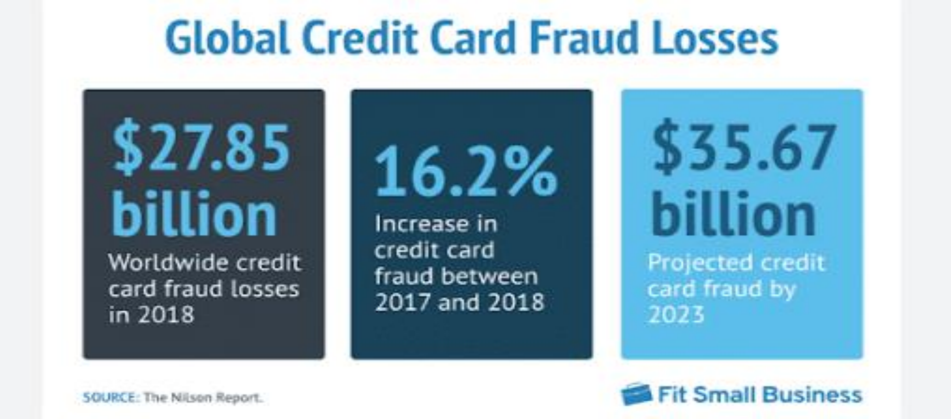
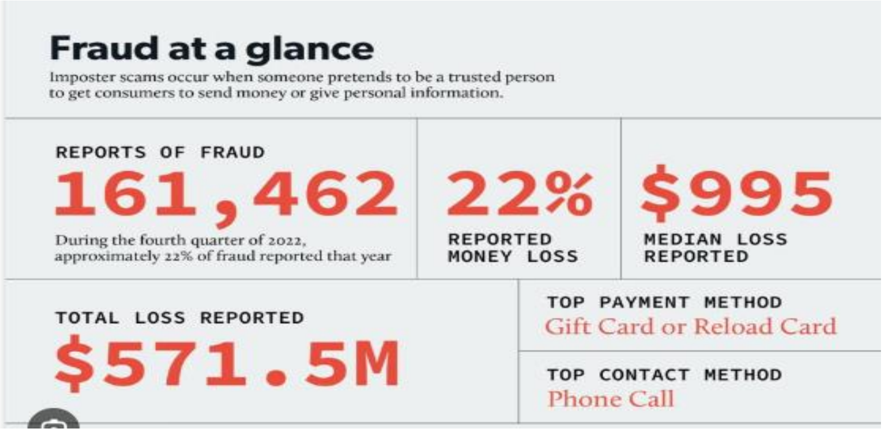


Fig 1: Worldwide credit card scam damages

(source https://cybeready.com/comprehensive-guide-to-fraud-detection-management-and-analysis/top-10-credit-card-fraud-detection-solutions-in-2023)



Fraud at a glance

Imposter scams occur when someone pretends to be a trusted person to get consumers to send money or give personal information.

REPORTS OF FRAUD
161,462
During the fourth quarter of 2022, approximately 22% of fraud reported that year

22%
REPORTED MONEY LOSS

$995
MEDIAN LOSS REPORTED

TOTAL LOSS REPORTED
$571.5M

TOP PAYMENT METHOD
Gift Card or Reload Card

TOP CONTACT METHOD
Phone Call

Fig 2: Scam at a glimpse

(source https://dailyillini.com/news-stories/champaign-urbana/2023/03/18/credit-card-fraud-cu/)

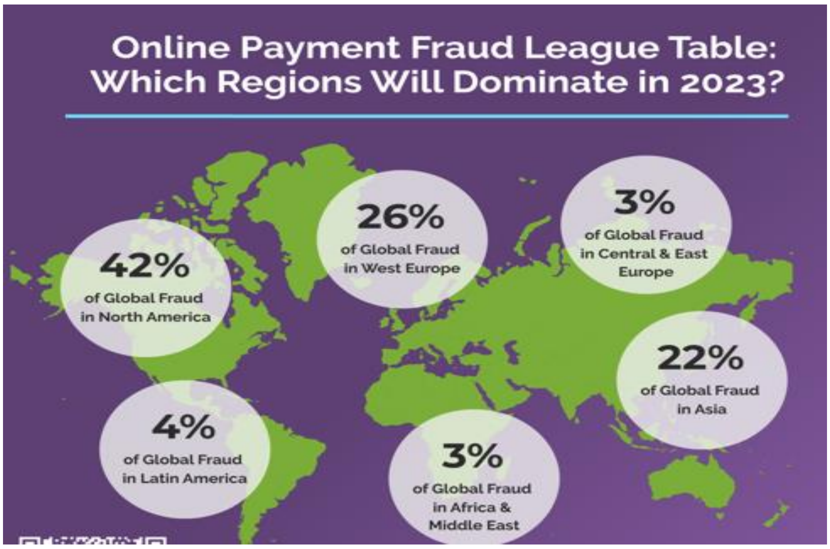

Online Payment Fraud League Table:
Which Regions Will Dominate in 2023?
42% of Global Fraud in North America
26% of Global Fraud in West Europe
3% of Global Fraud in Central & East Europe
22% of Global Fraud in Asia
4% of Global Fraud in Latin America
3% of Global Fraud in Africa & Middle East

Fig 3: Online transaction loss snapshot
(soruce: https://www.juniperresearch.com/press/ecommerce-losses-online-payment-fraud-48bn/)

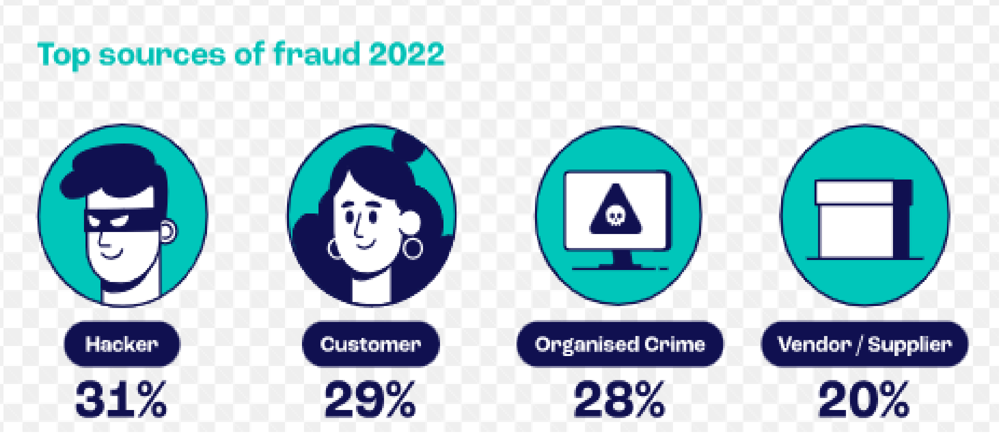


Fig 4: High priority of users details collections
(https://seon.io/resources/fraud-detection-and-prevention/)

II. EXISTING SYSTEM

- Online transaction password in not secure.
- Hackers can easily access the transaction details.
- No security.
- Customer do not want to change the secrete number provider by the bankers.
- Number are not change long period of time.
- Using the card for repetitively in the same locations without changing the four digit secret code.

Draw back of the existing system:

- Easy to predict.
- There is no proper security mechanism.
- It is easy to trace the four-digit pin number.
- Card details are explained to everyone.
- Number of visible.
- There is no security awareness.

III. PROPOSED SYSTEM

- In the proposed system, the one-time authentication is time-based; the secret number is validated for only a limited period of time,
- Utilizing Rich Reliability Alphanumeric Creation.
  This provides very secure transactions when using credit cards.
  • Two-step authentication is initiated for each transaction, requiring users to follow this procedure.
  • Users will receive an alert message after the second wrong attempt.
  • It is difficult to guess the randomly generated authentication code.
  • Each second step of authentication is generated by a different server.
  • Hackers are unable to predict the network flow of the transactions

Advantage of proposed system:

- Rich Reliability Alphanumeric Creation (RRAC) is utilised for authentication purposes.
- RRACs are generated randomly by different servers.
- Hackers are unable to predict the transactions.
- The same user conducting multiple transactions will receive different secret numbers.
- User credentials are stored in a highly secured database.
- Each time, users are required to undergo two-step authentication.
- Time-based authentication is implemented.
- Card details are securely stored.

IV EXPERIMENTAL SETUP:

Today, most transactions are happening online, allowing users to purchase or sell products via the internet. They can pay or receive amounts through online payment gateways using net banking or card-based transactions. This opens up opportunities for hackers to obtain user details in various ways, motivating them to steal information during financial transactions conducted online. To address this issue, there is an urgent need for additional authentication during online transactions. Scams on this platform are increasing daily due to various factors, so enhanced security measures are necessary.

The proposed method, shown in the figure, involves a three-step authentication process. Every time a user initiates a transaction, they must go through these steps, ensuring operations are performed efficiently and safely without any delay. In the proposed architecture, users' information is initially collected and stored. Each time a user initiates a transaction, the system verifies the user's information before allowing them to proceed further. The entire process is divided into various modules, such as user demand, user receipt, generation of Rich Reliability Alphanumeric Text (RRAC), facility supplier, receiving the RRAC through a short text message, and the procedure for performing the entire process. This procedure provides enhanced security and ensures that hackers cannot obtain any user details.

Most payment gateways today are enabled with two-way authentication mechanisms. Each time a user enters their credentials, a random RRAC is generated and communicated to the user via a short text message. This information is generated randomly, ensuring that even if the same user continues the operation or initiates another transaction, they will never receive the same RRAC. This process is performed by the RRAC server using symmetric key authentication mechanisms. This information exchange is highly secure because the key is known only to the transaction creator and receiver. Any hacker attempting to steal the RRAC would have no clue as to which product the information pertains to. In our proposed method, this process is explained through a three-step mechanism. Normally, the service provider also provides a four-digit authentication code after the request is made from the sender's side. Once the first step of verification is completed, users are required to enter the service provider's authentication code. This code is generated randomly by the service provider each time a transaction is initiated by the user. Even if the same user performs multiple transactions on the same day, the generated code is different each time.

A. Procuring

The primary operation performed in online transactions is purchasing items. Initially, the user is allowed to browse different items on the seller's site and has the privilege to compare these items with other existing products. Once the user selects a particular item, they proceed to pay online. The user will receive a procuring invoice, which is sent either via email or text message based on the credentials provided in step 1. After receiving this invoice, the user initiates the payment process. The user's request is then converted into a procuring order, and the payment for the item is initiated. This process is show in the fig5.

B. Consumers Ultimatum

Technology allows users to order items online with a single click, providing flexibility but also introducing unsecured transactions. Each time a user makes a purchase, they need to enter their credentials on the seller's portal. By knowingly or unknowingly sharing their personal information, users risk exposing their credentials to outsiders. This can lead to various misuses of financial information, as user details may be used by different vendors on various platforms. Additionally, users often receive fake calls claiming to be from service providers requesting their details. Another common method of information collection is through discarded items. Many customers throw away their credit card bills or transaction receipts without properly tearing them, allowing hackers to easily collect details. Sometimes, users forget to collect their bills or refresh the process while shopping, which enables hackers to gather customer credentials. This type of information is typically stored in sellers' databases, and hackers may pay sellers to obtain these details. Users have no control over their information once it is stored online. Such information can be widely shared and used by different vendors. This process is shown in the fig 6

C. Consumers Acceptance

This process will take care of items ordered by different customers in various locations. Each ordered item is received by the central system. The system records each item, the number of items ordered by the customer, the customer's location, and any discounts if a bulk order is received. All the information is updated with the help of the central system. This system will manage the entire order information across the network, updating the respective customer or distributor based on the item descriptions and availability.

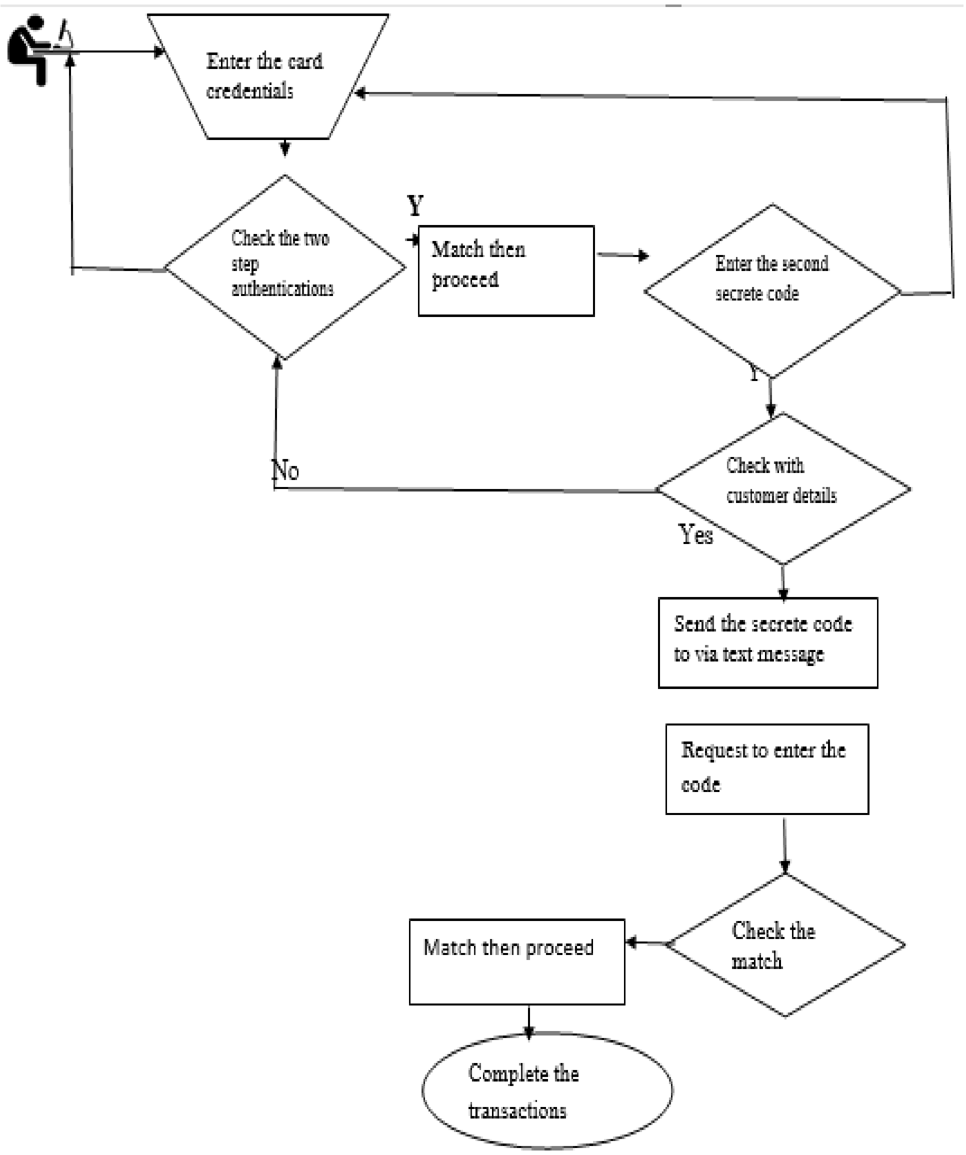

Enter the card credentials
Check the two step authentications
Y
Match then proceed
Enter the second secrete code
Y
No
Check with customer details
Yes
Send the secrete code to via text message
Request to enter the code
Check the match
Match then proceed
Complete the transactions

Fig 4: Proposed Architecture

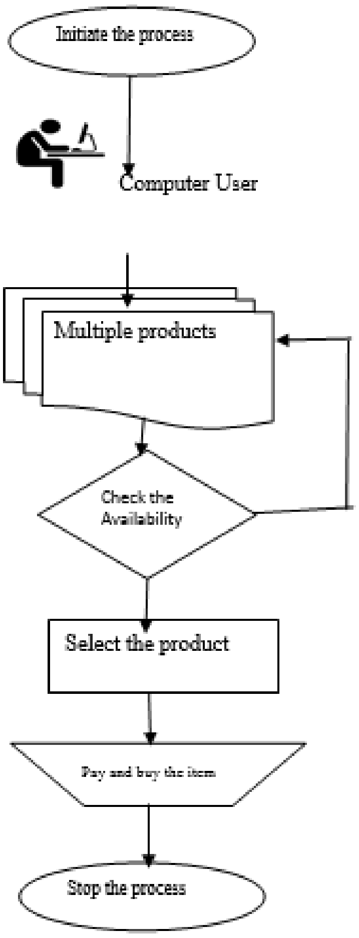


Fig 5: Stage-1 Authentication System Flow

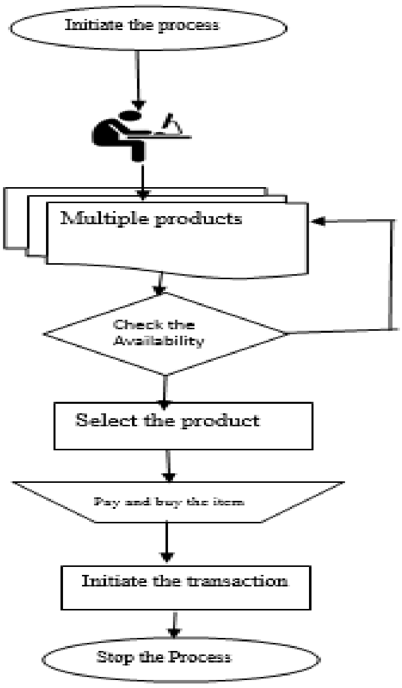


Fig 6: Stage-2 Authentication System Flow

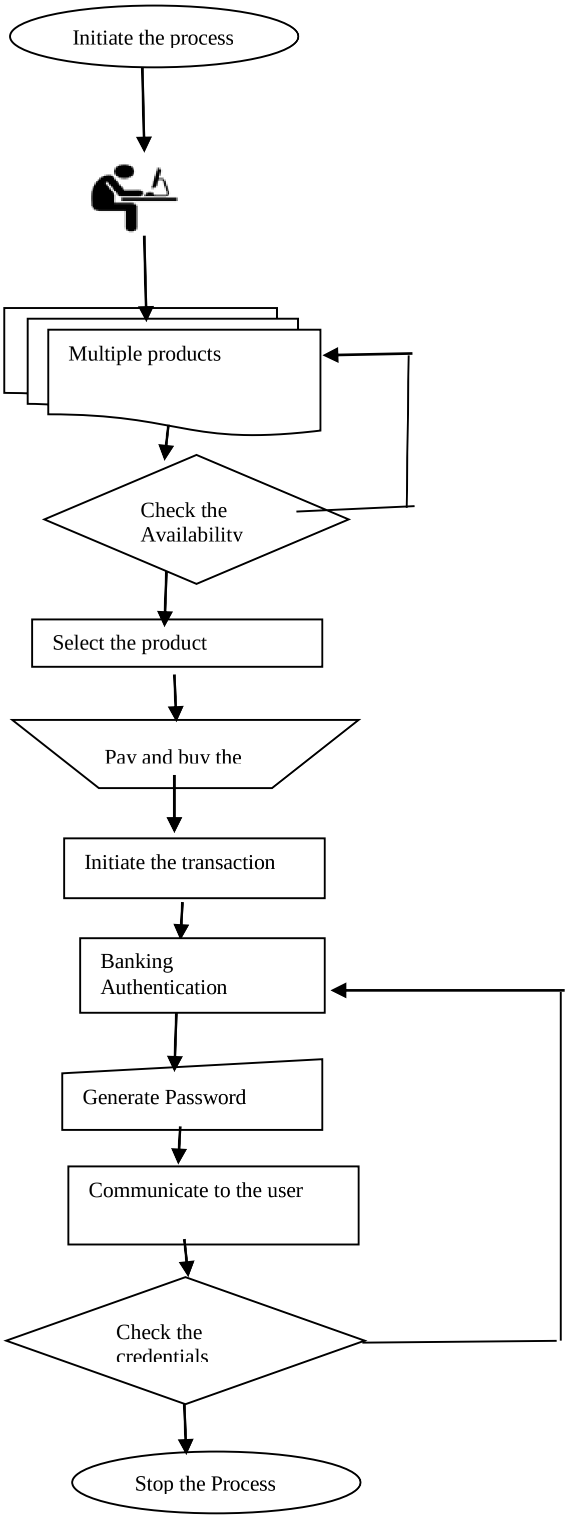


Fig 7: LEVEL-3 Authentication System Flow

D. Generation of Rich Reliability Alphanumeric creation

The entire process is divided into various modules, such as user demand, user receipt, generation of Rich Reliability Alphanumeric Text (RRAC), facility supplier, receiving the

RRAC through a short text message, and the procedure for performing the entire process. This procedure provides enhanced security and ensures that hackers cannot obtain any user details. Most payment gateways today are enabled with two-way authentication mechanisms. Each time a user enters their credentials, a random RRAC is generated and communicated to the user via a short text message. This information is generated randomly, ensuring that even if the same user continues the operation or initiates another transaction, they will never receive the same RRAC. This process is performed by the RRAC server using symmetric key authentication mechanisms. This information exchange is highly secure because the key is known only to the transaction creator and receiver. Any hacker attempting to steal the RRAC would have no clue as to which product the information pertains to. In our proposed method, this process is explained through a three-step mechanism. Normally, the service provider also provides a four-digit authentication code after the request is made from the sender's side. Once the first step of verification is completed, users are required to enter the service provider's authentication code. This code is generated randomly by the service provider each time a transaction is initiated by the user. Even if the same user performs multiple transactions on the same day, the generated code is different each time.

Several methods for the generation of Rich Reliability Alphanumeric Text (RRAC are registered under:

- In Method One, each time a user registers for login or performs any transaction, they receive a four-digit text-based authentication code. This code is randomly generated and shared with users based on a time duration. This means the given authentication is validated only for a specific period. Once the time elapses, the code is automatically invalidated, even if it has not been used. This method is highly secure within the proper time limit. After the user has verified the code within the stipulated time, a second authentication is done based on time validation, requiring the user to enter the authentication code within the set timeframe.
- The entire process is controlled and performed by three different servers. The first server checks the user's credentials, verifying if the user is valid. After validation, the second server checks the first step of the process, which involves the authentication service of the registered user. If the user is validated, they can continue their operations. After this process, the random generation service is initiated. Each time, the user receives a randomly generated password using different combinations, so the user has no clue or idea about these random numbers. If the user wishes to continue the same operations at the same time, the information is not repeated; new numbers are generated each time. Sometimes the numbers are generated based on a mathematical model, using certain calculations to produce the random numbers that are then shared with the user to complete the operations.

The authentication generated by the server is done through different mechanisms. In the first method, each time the user initiates any transaction or login process, the service provider randomly generates and circulates a four-digit password to the user. Each time the user performs a transaction within the same period, they will never receive the same number; each transaction is treated separately and receives a new authentication number. This improves security, as neither the user nor a hacker will have any clue about the number they will receive at the time of the transaction. It is a highly secure mechanism to prevent hacking. In the second method, the procedure-oriented system involves every user's mobile, which contains a special procedure that takes care of the transaction. Whenever the user generates any operation, this procedure controls the process and generates a new token. For each transaction, the user receives a new token, which they have no prior knowledge of.

E. Facility supplier

During financial transactions, most service providers or payment gateway authorities act as mediators between the client and the banks. They collect information and check the credentials of the users. After this process, they generate an invoice and send it to the user to pay the invoice amount using any payment gateway method, such as net banking or UPI. The service provider collects the invoice amount and sends it to the banks. The amount is then debited from the user's account, and a confirmation message from the bank is communicated to the user. This way, the entire transaction is monitored and controlled by the service provider, who may charge a nominal fee for these operations. For initiating this type of transaction, nowadays, transactions are completed via debit or credit card through various service providers. Most payment gateways today are enabled with two-factor authentication mechanisms. Each time a user enters their credentials, a random Rich Reliability Alphanumeric Code (RRAC) is generated and communicated to the user via a short text message. This information is generated randomly, so even if the same user initiates another transaction, they will never receive the same RRAC. This process is performed by the RRAC server using symmetric key authentication mechanisms. This information exchange is highly secure because the key is known only to the transaction creator and receiver. Any hacker attempting to steal the RRAC would have no clue as to which product the information pertains to.

These transactions are done through debit or credit cards. Today, these cards are enabled with an electronic chip that contains the customer's credentials, eligibility, and link with the service provider. The card performs two types of functions when the customer uses it for any financial operations. Initially, when the customer swipes or uses the card, it checks if the card is valid. After this initial process, it requires first-stage authentication, where the user needs to enter the four-digit secret code provided by the service provider during card registration. Each transaction’s first step is validated against the information provided at the time of registration. After this validation, based on the operation, the user proceeds to the second step of the verification process. Each time the card is swiped against the machine, the two-step verification process is conducted, and only then is the transaction completed. After the first step is completed, a random Rich Reliability Alphanumeric Code (RRAC) is generated and communicated to the user via a short text message. This information is generated randomly, so even if the same user initiates another transaction, they will never receive the same RRAC. This process is performed by the RRAC server using symmetric key authentication mechanisms. This information exchange is highly secure because the key is known only to the transaction creator and receiver. Once this process is verified, the user gets a confirmation from the service provider. Whenever the user performs operations, this two-step process is initiated and completed each time, even for the same type of operations or transactions. This process never reveals any clues, ensuring that neither the user nor others get any information about the operations. If a hacker tries to steal any packets or information during the transaction, the information is received from three different servers, making it impossible to determine from where the information is received. Therefore, the entire transaction process is highly secure and safe.

F. Receiving RRAT through text based source

The entire operation is initiated and controlled by various devices nowadays, with the most popular device being the mobile phone. The phone's information is initially collected and verified by the service provider. Each user is assigned a unique customer identification number. Each time a transaction starts, the service provider checks the credentials against the customer identification number before allowing the operation to continue. Each time, the user receives a secret code or four-digit high-security code via an alphanumeric text message. This code is validated by the service provider, enabling the user to enter the information and complete the operation. This information is received by the user's mobile phone with the help of the mobile phone network provider. These codes are initially shared and received by the network provider but are sent in an unreadable format. Once the information is received by the user, it is converted into a readable format using a conversion mechanism. This ensures that if a user or hacker tries to steal the information in transit, it remains secure and unreadable. If the user is out of their home area, this information is shared via various service providers, sometimes involving more than two or three network providers. At any time, the information is highly secured and converted into an unreadable format. Only once it reaches the customer's device is it converted into a readable format. The two-step verification and authentication depend on the device used by the user. Every device is capable of generating the secret code, and these codes are highly protected. If a user's mobile gets damaged or stolen, the user can immediately report it to the service provider, who will stop sending secret information to that particular device.

Algorithms Used

The RRAC procedure is the basic method used only in the user and service provider side functions. These values are known only to these two authenticated parties; the third party does not have any clue about these operations during the transactions. To perform the RRAC, the procedure is shown below. The generated outcome has a high value, so this value is reduced to eight bits of code. Each time this procedure is necessary, it fits into the device. This step is shown. Create the EVENT EXECU value. Let RRACK = EVENT EXECU (Value, E); RRACK is a 30-byte sequence. Here, the long-bit code is converted into smaller bits without loosing its originality.

The procedure can be designated in 3 stages:

Stage 1: Create the EVENT EXECU value Let RRACK = EVENT EXECU (Value, E) // RRACK is a 30- byte sequence

Stage 2: Create a Conversation cypher of the RRAC EVENT EXECU= ToRRAC (RRACK).

Stage 3: Mine the secrete RRAC assessment from the sequence RRAC=Trim (RRAC. RRACK)

Procedure

```
Communication Condensation CC = Communication Condensation ("AAFD")
CC.apprise(Value,E)
Productivity = CC.Alphanumericset()
Temp = hexstring((productivity >> 8) & 0AOx)
RRACK=Temptobyte sequence()
RRACK=RRACK.byte.sub sequence(0,8)
```

In the increasingly digital world, the necessity of an authentication process for any operation is crucial because transactions are performed by different users in various locations. Each time, authentication ensures that communication is conducted with authorised users. This validation guarantees that the transaction is performed by an authenticated person or system, providing additional comfort to the user community. Technology allows users to connect from different localities, and only this authentication ensures the smoothness of the transactions. Today, users from diverse backgrounds perform transactions digitally using the internet as the medium. In such cases, a more robust authentication mechanism is required to complete the transactions. The proposed system for a two-step verification process is highly secure. Each time, the user receives a random secret number, providing more authentication and security for the transactions. The entire process is controlled and performed by three different servers. The first server checks the user's credentials, verifying if the user is valid. After validation, the second server checks the first step of the process, which involves the authentication service of the registered user. If the user is validated, they can continue their operations. After this process, the random generation service is initiated. Each time, the user receives a randomly generated password using different combinations, so the user has no clue about these random numbers. If the user wishes to continue the same operations at the same time, the information is not repeated; new numbers are generated each time.

V. EXPERIMENTAL OUTCOME

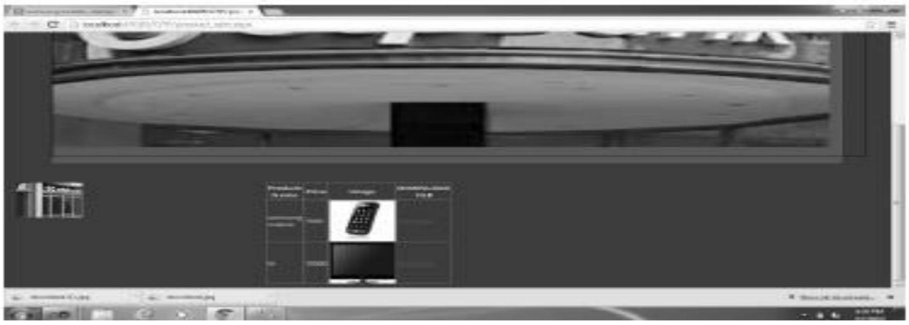


Fig 8: Merchandise Procedure

Fig 9: Ingoing operator keyword

Fig 10: Ingoing Client Particulars

Fig 11: Creating Rich Reliability Alphanumeric Code

VI. DECISIONS AND UPCOMING IMPROVEMENT

The proposed method, shown in the above involves a three-step authentication process. Every time a user initiates a transaction, they must go through these steps, ensuring operations are performed efficiently and safely without any delay. In the proposed architecture, users' information is initially collected and stored. Each time a user initiates a transaction, the system verifies the user's information before allowing them to proceed further. Each transaction is treated separately and receives a new authentication number, ensuring that the user never receives the same number within the same period. This enhances security, as neither the user nor a hacker will have any clue about the number they will receive at the time of the transaction. It is a highly secure mechanism to prevent hacking. In the second method, the procedure-oriented system involves every user's mobile, which contains a special procedure that takes care of the transaction. Whenever the user initiates any operation, this procedure controls the process and generates a new token.

A one-time password RRAC (Rich Reliability Alphanumeric Code) solution offers two-factor authentication using something you know, such as a secret code, which is communicated to the user's device via the RRAC procedure. As their label suggests, RRAC is validated only once during the transaction period. If the user continues the operations, they will receive new random values. RRAC avoids many shortcomings associated with outdated fixed passwords, the most significant being that RRAC does not provide any clue or hint to users. In other words, even if an RRAC is stolen, it can only be used once. RRAC solutions are ideal for companies where a remote workforce needs access to resources such as networks, mail, and web pages. They are especially useful when these resources are accessed through the Internet or an intranet.

References

1. https://cybeready.com/comprehensive-guide-to-fraud-detection-management-and-analysis/top-10-credit-card-fraud-detection-solutions-in-2023.
2. https://dailyillini.com/news-stories/champaign-urbana/2023/03/18/credit-card-fraud-cu/.
3. D.Saravanan, Dr.S.Srinivasan, (2013). , Matrix Based Indexing Technique for video data, Journal of computer science, 9(5), 2013, 534-542.
4. D.saravanan, Dr.S.Srinivasan (2012). Video image retrieval using data mining Techniques, Journal of computer applications (JCA), Vol V,Issue 01, 2012. 39-42.
5. D. Saravanan,” Scholar Attendance monitoring using one time keyword generation technique" Manger – The British Journal of Administrative Management, Volume 58, Issues 148, March 2022, ISSN:1746-1278, Pages 165-171.
6. R. Jaques. Identity theft worse than Iraq war. Available from: http://www.vnunet.com/News/1140291.

7. Private Payments locked with smart chip. Available from:http://home4.americanexpress.com/blue/privatepayments/spla sh.asp.

8. D.Saravanan, A.Ramesh Kumar, “ContentBased Image Retrieval using Color Histogram”, International journal of computer science and information technology (IJCSIT), Volume 4(2), 2013, Pages 242-245, ISSN: 0975-9646.

9. https://www.juniperresearch.com/press/ecommerce-losses-online-payment-fraud-48bn/

10. D.Saravanan, Dr.S.Srinivasan(2013) “Video information retrieval using :CHEMELEON Clustering” International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),Volume-02,Issue 01, January –February 2013, Pages 166-170.

11. D.Saravanan, Dr.S.Srinivasan (2011). A proposed new Algorithm for analysis for analysis of Hierarchical clustering in video Data mining, international journal of Data mining and knowledge engineering, vol 3, no 9.

12. A.D. Rubin and R.N.Wright. Off-line generation oflimited usecredit card numbers. In: Proceedings of Financial Cryptography, 2001, pp. 196–209.

13. A. Shamir, Secure click: A web payment system with disposable credit card numbers. In: Proceedings of Financial Cryptography, 2001, pp. 232–242.

14. D.Saravanan, KVSSN Narasimha Murty, Image frame Evulsion using data mining clustering Approach”, Empirical Economics Letters, 20(special issues 1), June 2021, Pages 87-91, ISSN:1681-8997

15. D.Saravanan,V.Somasundaram “Matrix Based Sequential Indexing Technique for Video Data Mining” Journal of Theoretical and Applied Information Technology 30th September 2014. Vol. 67 No.3

16. https://seon.io/resources/fraud-detection-and-prevention/