Research Article

Efficient Encryption mechanism for financial transactions: Avoiding data loss and tackling collisions

Damanpreet Kaur[1], Kiranbir Kaur[2]

[1]Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar
[2]Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract

Security in financial transactions is a necessity. This security is provided using various encryption mechanisms such as RSA, DES, AES, and hybrid encryption mechanisms. The problem, however, arises when financial transactions take place in the banking sector. This paper proposes a unique DNA-based block chaining to avoid any collision and to provide a high-end security during financial transactions. The block chaining mechanism provides a two-way security during financial transactions along with avoading data theft, as well as data loss, is avoided. The implementation results of the proposed system are presented in terms of throughput, encryption time, and decryption time. The results obtained for the encryption and throughput, are optimized using this approach, however, encryption time still requires certain modifications. The overall results are better than Changsong et al., 2020.

Keywords: Block chaining, collision, DNA encryption , Tags, authentications

Introduction

When bank users do transactions or performed operations like deposit, withdrawl, RTGS or NEFT then the security is provided by the block chaining. Every bank user is given a unique username and password and for security purposes one time passwords are availed for overall transactions. A two-way authentication mechanism is used i.e bank users are provided with a unique address which is associated with the userspace. It indicates that userspace will be accessed only if both the username and password alongwith the OTP verifications. Then data stored uses the encryption and decryption method. The data stored within the block is first encrypted, and decryption is needed to access the data. The following figure describes the authentication mechanism used by banking systems.

Figure 1:Two factor authentications

Server end will verify the authentication mechanism. The user will be given three attempts and will need to contact the banking service provider if they reach that amount. The next segment goes into the financial and banking sector's mechanisms.

Block Chaining in Finance

To address the growing needs of users, block chaining uses a distributed database, while conventional financial systems use a centralised database with a single point of authority. Without depending on a single authorization system, a user with proper authorization may access records from multiple systems. The smart contract, which is a self-executing protocol that enforces a previously negotiated agreement, is a key feature of block chain. For example, a smart contract might automatically initiate a refund if certain conditions are met, or it could initiate automatic payment of credit card bills on the due date. As indicated by, block chain has a number of advantages (KPMG, 2019).

- From a single server, the error rate caused by ledger synchronisation is reduced by 95%.

- Straight through processing and single source of truth increase the efficiency.
- Processing speed, customer experience is improved by using digital channel.
- Capital demand is reduced as transactions are settled faster and capital defects are freed up.

Block Chaining in Banking

The use of a block chaining tool is accompanied by the assignment of a particular person to ensure the customer's privacy. In block chaining multiple security plan are applicable to closed the information within the block as the financial detail need to sort the security. This block chaining technique in banking is divided into two main sections. Figure 2 depicts the phases of block chaining used to secure bank transactions.

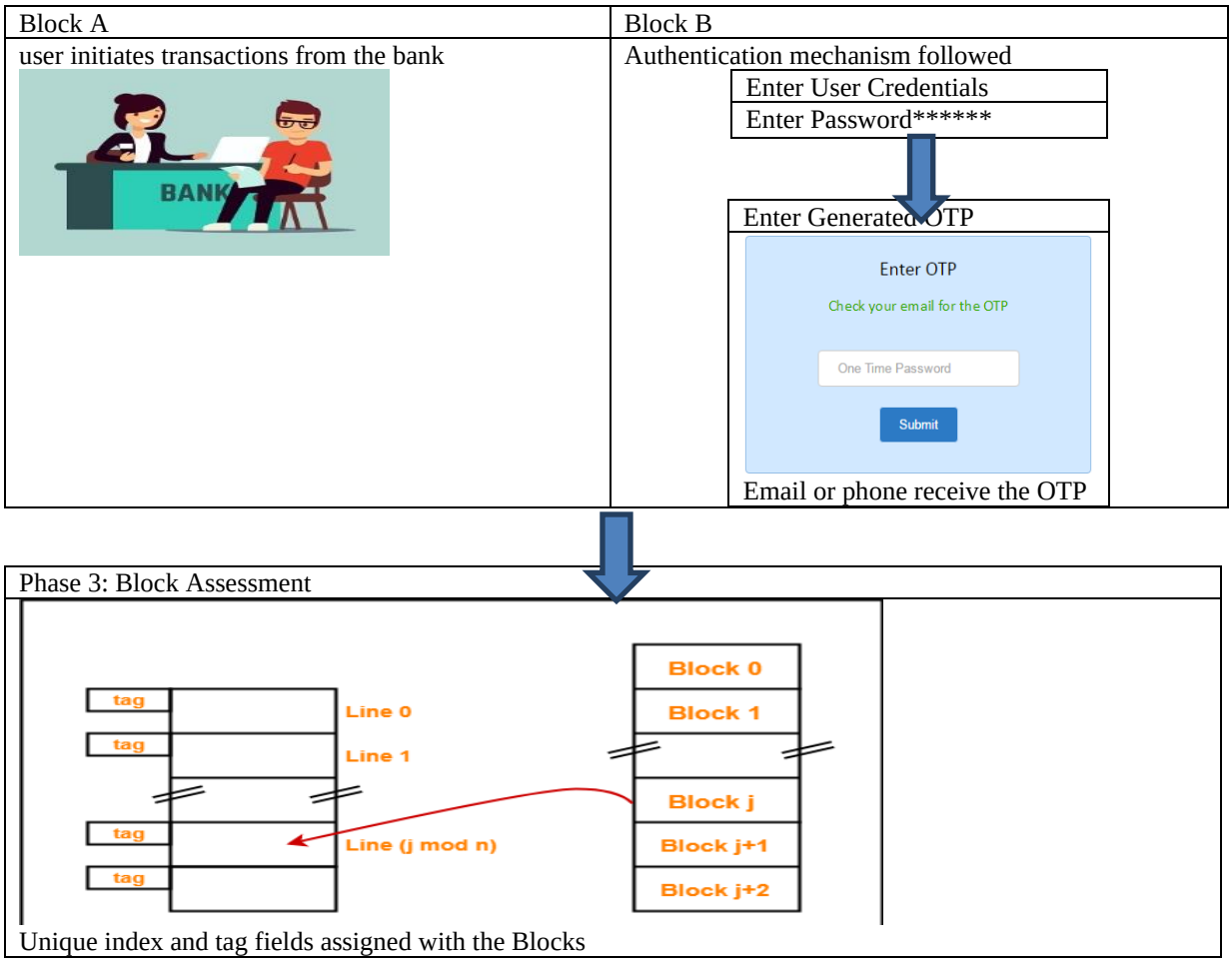

Figure 2: Procedure based on block chaining in Banking

Firsty the login activity is initated by the user after infiltrate User Credentials and password. For two-way authentication the listing mobile number is used. Formely the OTP is infiltrate by the customer, access to the blocks will be allowed in encrypted and then it requires decryption key. A decryption key is required to access the information block.

A secured tool is related within the block chaining yet similar index for multiple customers could be give rise to collision. Collision issue is infrequent still could arise in case of heavy traffic that can be sort out using the proposed mechanism.

Collision problem

Collision is a problem that causes the overlapping of blocks which may overwrite the information of an existing user within the block. The overall address generation process is described via the given Table 1

Memory Address	Data
11111	101 X1Y1Z
71111	201 A1B1C1
--	--
---	---
11666	130 X1Y1Z
70666	140 A1B1C1

Table 1: Representation of memory in multi block chain approach

Memory address correlate to five dissimilar bits. The first two bits represent the tag and the remaing 3 bits indicate the memory address. Similar index illustrate accounts of the similar user. Same index lead to overlapping the account deatail of user just one account detail will be saved. In order to reduce this collision problem multiple tag is used. The frame of suggested mechanism is shown in figure 3

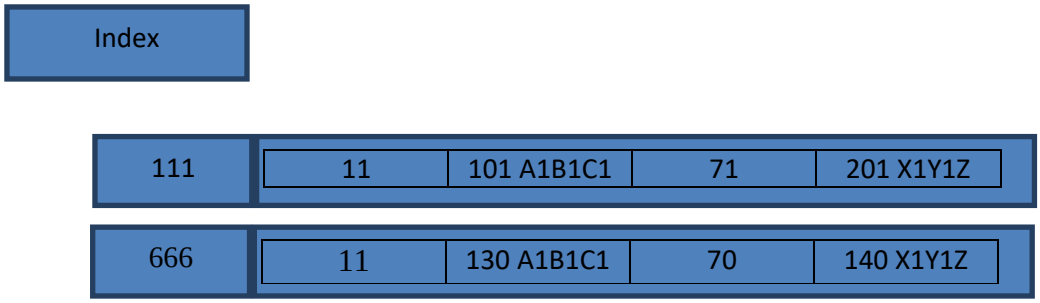

Figure 3:Suggested mechanism follow the given structure

By using this frame work, , similar index field would carry multiple detail blocks.

Related work

This section summarises the research that has already been done on banking transaction security. The following is a list of some of the work that has been done in this field.

In Banking Sector

An independent digital currency block chain mechanism was proposed by (Tsai et al., 2017). The guidelines for block chaining were implemented, including protocols, database design patterns, and chain code used in the process, as well as the flaws. To ensure copyright rights and digital payment, algorithms such as account block chain and trading block chain are used. Conclusions: The Beihang chain was designed to provide a secure environment for data storage within blocks. Customer confidence and reliability increased as security standards improved.

In the banking sector, (Guo and Liang, 2016) suggested a security enhancement system based on block chaining. The overall process for forming a block is determined by the number of users and accounts they have. Since multiple accounts cannot be managed using this method, each block corresponds to a single user. Computations: are a block chaining method for storing data for multiple users. Conclusions: Block chaining ensures that user transactions are reliable. This mechanism has the potential to dramatically improve trust levels.

(2019, Li) The implementation areas of block chaining were discussed. In the field of defence, block chaining is thought to be a new technique. Other protection mechanisms such as RSA, DES, and DNA encryption were compared to this mechanism. Computations: DNA encryption, RSA, DES, and block chaining are examples of algorithms. Conclusions: Despite the fact that block chaining is safe, each block must be encrypted. It was discovered that DNA-based encryption was superior to the RSA and DES approaches. As a result, DNA encryption combined with block chaining will improve transaction security.

The block chaining mechanism for ensuring transaction stability was addressed by (Rega et al., 2018).Before being transmitted, transactional data must be secured. This encryption method was combined with a block chain based on the creation of a single tag. The address structure is made up of five distinct bits that make up the name. The first two bits function as a tag, while the remaining bits function as an index. Computations: The algorithm is block chaining tag creation with transactional security. Conclusions: The security of the transaction has improved, as shown by the reliability factor. To improve security, this investigation can be combined with multiple tags and DNA encryption.

In Communication Protection

During contact, (Beeputh, Doomun, and Dookee, 2010) suggested an energy conservation protection framework for wireless sensor networks. The packets sent to the destination have an effect on the network's lifespan. Block chaining with the AES encryption method was suggested to reduce the amount of energy consumed as a result of unauthorised attacks. The algorithm is Block Chaining with AES encryption.Conclusions: With this approach, energy is conserved while still ensuring transmission security.

According to (Stallings, 2010), block cypher protection can be used to ensure confidentiality. For the users, the information transmitted over the network could be critical. Unauthorized access could impede communication

efficiency, so a protection framework based on block chaining was proposed to address this issue. In communication, an algorithm is a block chaining mechanism. Conclusions Primary formation transmission reliability and execution time

(Sahi, Lai, and Li, 2018) suggested using a block chaining mechanism in communication to ensure security. The user's data was contained within the block. And this block is encrypted, which means that each block has its own decryption key. This method also ensures that data protection is maintained when decryption is supported by several keys. Block chain is an algorithm for increasing the protection of user transactions. Conclusions: Encryption execution time increased as reliability increased. Multiple tag support was lacking in the analysis.

Comparative analysis

References	Techniques	Merits	Future Enhancements
2016 (Guo and Liang)	Inside the banking sector, disable encryption.	Block chaining increases protection since each user block is secured with a unique key.	Since multiple tag support isn't available, each user can only handle one account.
(Hu and colleagues, 2019)	Transactions are conducted using a delay-tolerant approach.	Short message based service is used in remote areas where internet connectivity is a problem. On the other hand, this service contains a security threat that is addressed in this way.	This approach cannot protect users who have multiple accounts.
(Arora et al., 2017)	The RSA algorithm is used to secure the cloud through an ecosystem mechanism.	Encryption of data contained inside datacenters ensures security and privacy.	Public key encryption is not without flaws, and it necessitates the inclusion of additional authentication and privacy-preserving mechanisms.
2017 (Malik, Singh, and Narain)	The RSA algorithm is used to secure the cloud.	The RSA algorithm is a symmetric public key algorithm that provides cloud security.	Since it is public key encryption, it is slow. Multi-tag support is needed to improve the functioning of the system.
(Sivanathan and colleagues, 2016))	IoT-enabled smart homes need a low-cost security system.	Implementing security mechanisms is expensive and time-consuming. This mechanism, on the other hand, ensures fast encryption and is also cost efficient due to low bandwidth usage.	There is no support for multi-level authentication. As a result, tag support is needed, as well as a more secure mechanism.

Table 2: Comparative analysis

Data Validation and Proposed Methodology

The data validation process ensures that the user proposed transaction chosen file is in an accessible format. Only text files in the txt, pdf, and docx formats should be selected for encryption. To complete the operation, the following files should be loaded.

In order to perform better classification and encryption, data validation ensures that the uploaded data is correct. The process that makes use of structured data is shown in the table below. After that, the file is imported, and clients of a similar nature are stored in the same index location as before, but with the addition of multiple tag support.

AC No.	Name(First)	Name(Last)	Account_Holder_Email	Sex	Ac_Group
1	Kanica	MacBarron	kbirt012@paypal.com	Female	4.9E+16
2	Nikita	Smith	narthey123@paypal.com	Female	5.6E+13
3	Ariena	Williams	aclapison212@miibeian.gov.cn	Female	3.77E+11
4	Siseley	Brown	sdummer315@miibeian.gov.cn	Female	3.57E+13
5	Spense	Johnson	smccourt454@youku.com	Male	3E+18

6	Lunus	Jones	ljasik578@prweb.com	Male	6.76E+19
7	Alfredea	Garcia	alinnit698@wisc.edu	Female	4.91E+14
8	Elvis	Lopez	atertre704@wisc.edu	Male	3.53E+12
9	Dixie	Gonzales	dtetla812@devhub.com	Female	3.56E+13
10	Aillyn	Thomas	asiddens925@weibo.com	Female	3.7E+15
11	Benet	Wilson	Blandmana876@microsoft.com	Male	3.59E+17
12	Horate	Ghidetti	Hdoogueb890@ telegraph.co.uk	Male	6.39E+19
13	Rutgerie	Joseph	Rghidettic456@microsoft.com	Male	4.51E+16
14	Vauvan	Paolazzi	Vmainstond367@ friendfeed.com	Male	6.76E+14
15	Rupci	Linnit	Rdemarse375@domainmarket.com	Male	5.49E+16
16	Fedric	Siddens	Ccasfordf432@friendfeed.com	Male	3.56E+18
17	Rodovico	Arthey	Lpaolazzig225@flickr.com paypal.com	Male	6.04E+17
18	Emog	Jackson	Emacbarronh789@flickr.com	Female	5.6E+15

Table 3: Uploaded dataset

The method that is used is determined by the multiple tag support provided by the proposed scheme. This model's encryption is DNA, which is the most reliable encryption method available. The following is the job process.

Algorithm

Multi-block chaining algorithm with multiple tags

- Check new client shown
  Set blk=new blk()
  Inside the block, keep track of transactions.
  Ptr2=first1 / ptr2 is a temporary variable, and first1 is the address with the first block.
  while(ptr2!=null)
  Ptr2=nxt[ptr2]
  then loop ended
  Ptr2=blk
  Blk->nxt=null
- check the client id for data updating
- Division method is used for generating keys

Track keys in storage space by using index and key called tag
Interrogate valid queries and security keys
Complete the decryption and show the data to the client.

There are two steps of this approach. New transactions and users are registered in the first stage, and a large amount of data is needed in the second stage to modify existing data. The data cannot be changed by an unauthorised person.

Methodology

This section described the methodology of proposed method shown in table 4

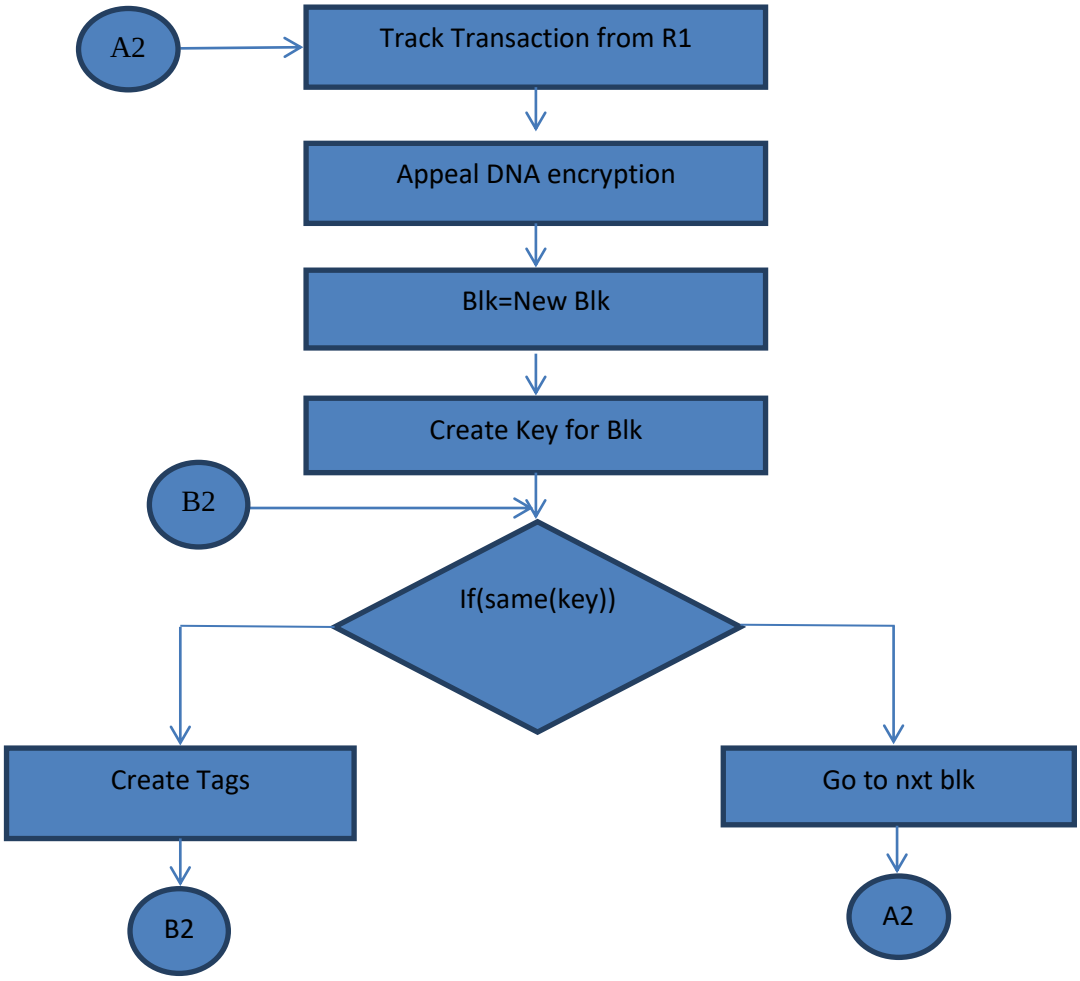

Table 4: Methodology

Description of the Methodology

The technique is broken down into two stages. The first transaction occurs. The procedure for recording is outlined below.

T1=Cust1_Transaction

Then encryption mechanism is applied.

Random prime numbers are used in the DNA encryption process. . Let uu=3 and vv=11.

Where

Uu denotes sender key length.

vv denotes receiver key length.

N2 denotes the size of the accumulated key from sender and receiver key.

No. of bits along with the final key is computed as shown below:

N2=uu*vv(Sender End) and ΦΦ =(uu-1)(vv-1)

Public and private key calculated

N2=3*11 and ΦΦ=(3-1)(11-1)

N2=33 and ΦΦ =20

The random procedure is run, and WW is run with the coprime domain. Then the factors generated ΦΦ by should not be divisible by RR. This approach does not divide by 5 or 2.

The value of RR may be 3,7,11,13, and so on. We'll go with WW=7. The values of DD for the private key are now determined as follows:

G1cd(ΦΦ,e)= ΦΦx+RRy

Where y=3 hence g1cd(ΦΦ,e)=1 therefore means value of PP=1 is right.

Then encryption and decryption are computed as under

$MM=N^{RR}ModN1$(At the encryption end)

$KK=B^{DD}ModN1$(At the decryption end)

Where MM=29 and KK=2. then encryption and decryption are computed.

Blk=New Blk

The key will generate a unique address within the block, producing the same result as a collision. To address this problem, the Sequential tag was developed. This tag will be incremented by one if a similar key for multiple blocks is generated. This tag will be incremented by one if the same key is generated for multiple blocks.

Experimentation and Evaluation

The experiment was conducted within Netbeans and cloudsim. The dataset was formed with .txt extension. The mechanism used provide multiple tag support. This was required to accomplish collision resolution. The multiple tag support block chaining mechanism construct a dynamic memory block formation. The block was separated using multiple tags corresponding to single index. This means index can support multiple data allocation corresponding to single user. This is not possible with single tag support. Collision problem was resolved using this mechanism.

Analysis of Results

When the simulation is run, this is the first window that appears. The user first selects the file and uploads it to the uploading section.

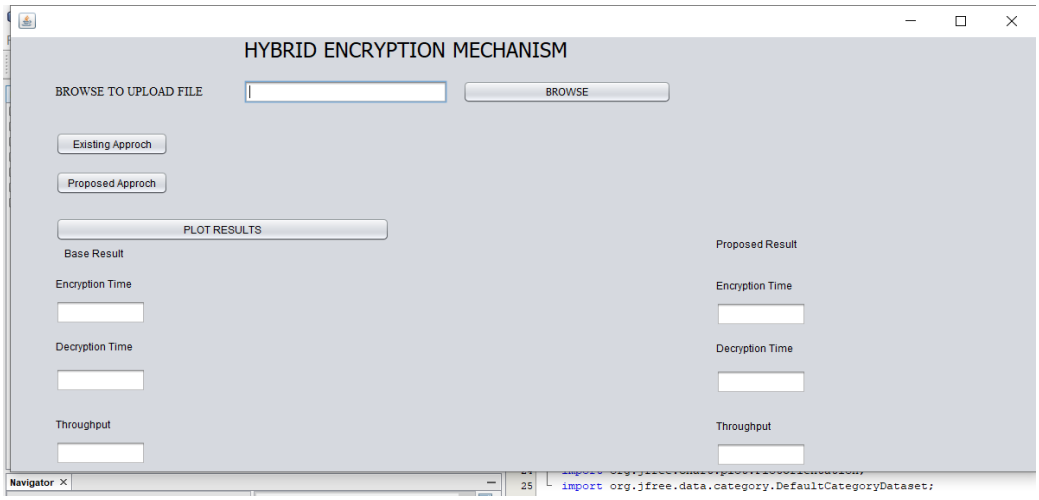

Figure 4: First window uploading file

To include the file name the selected file will be showed in the textbox.

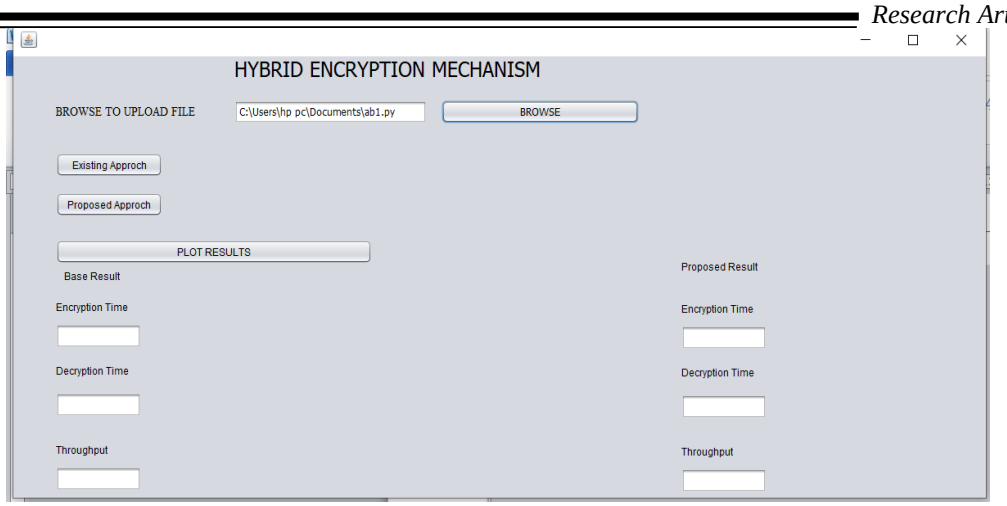

Figure 5: Selected file

When the user selects the current approach button, the desired result is shown in the textbox in the form of throughput and execution time, i.e. encryption and decryption times.

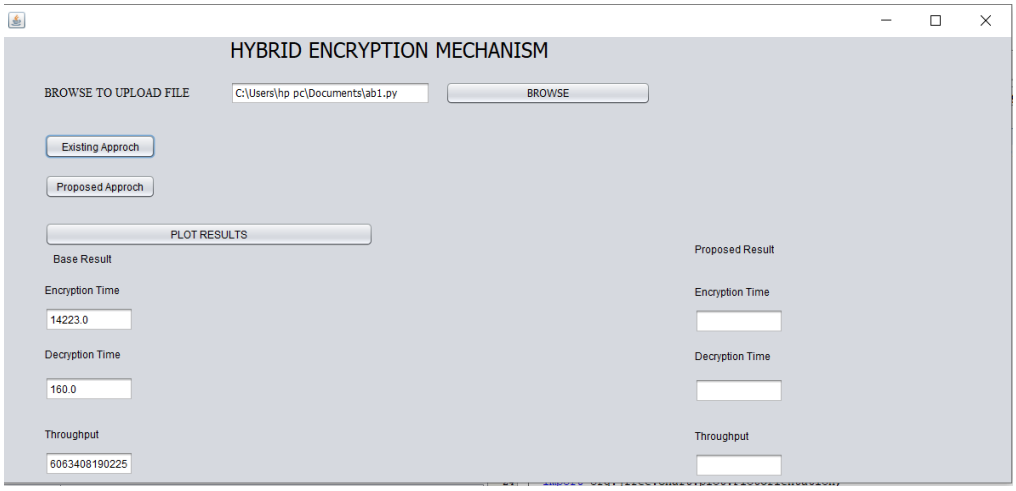

Figure 6: Encryption that works

When a user clicks on the proposed encryption button, the following image shows the effect. The encryption time is decreased when collision resolution is used, but the decryption time is increased.This is due to collision resolution that permits multiple tags for save and get information from multiple tags which results in more time.

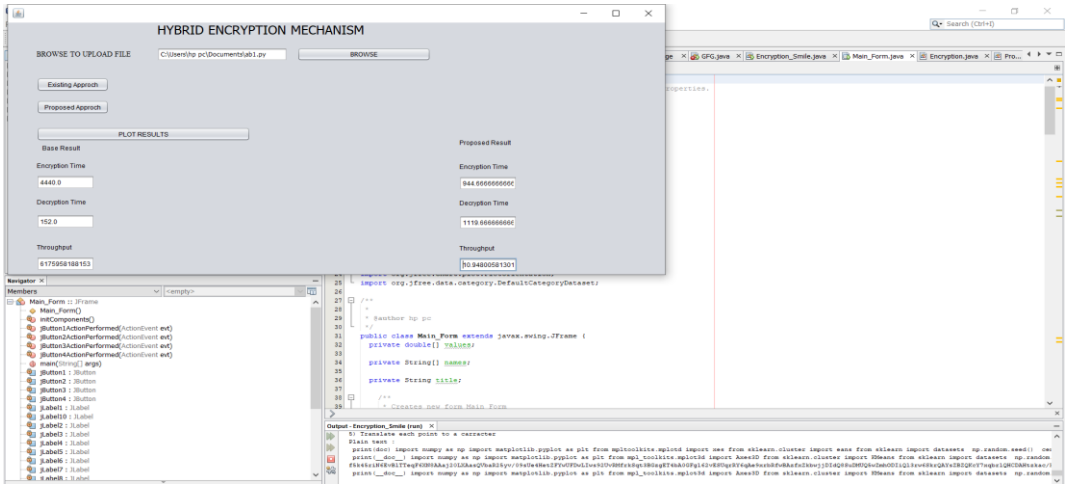

Figure 7: Suggested Encryption mechanism

The above stage are repeated again and another file is choosed for functioning.

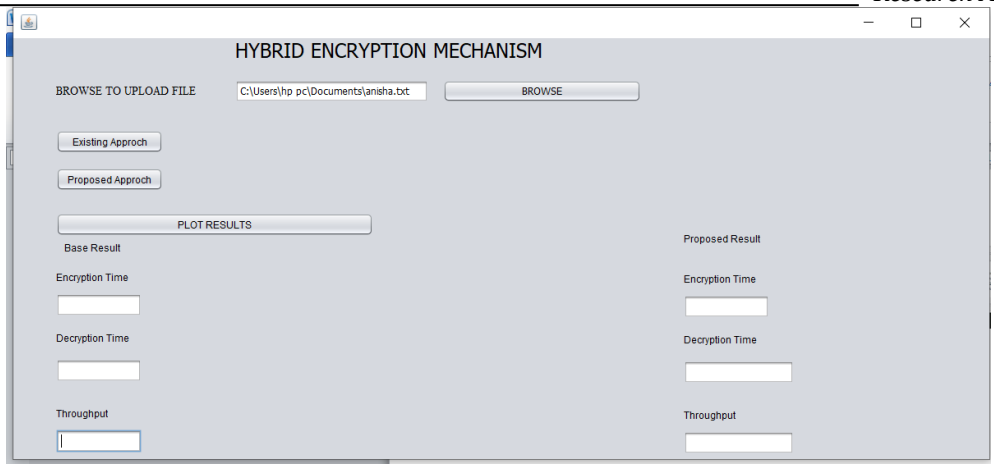

Figure 8: Choose another file

To generate encryption as well as decided blocks the user will click on the existing approach process after choosing the dataset. Every block are followed with the key for decryption.

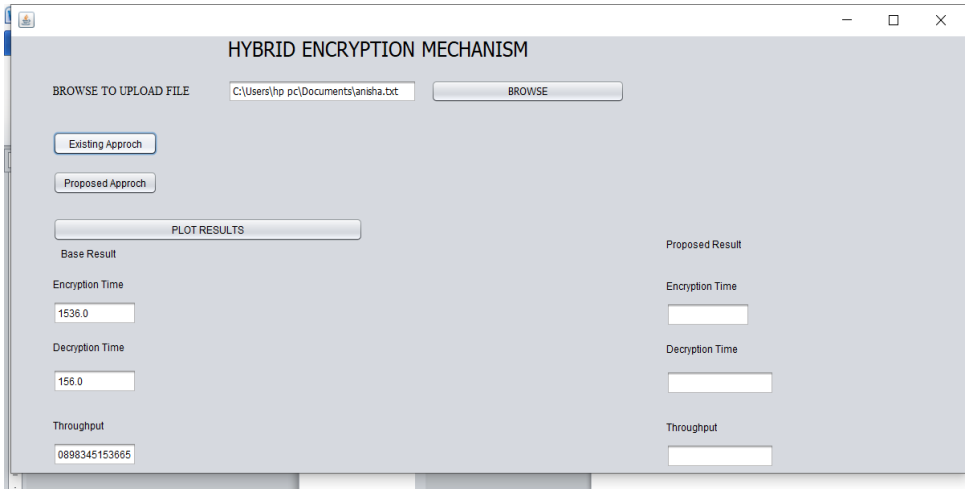

Figure 9: Result of existing approach

When the user clicked on proposed approach then the DNA encryption also collision resolution occurred that developed the blocks.

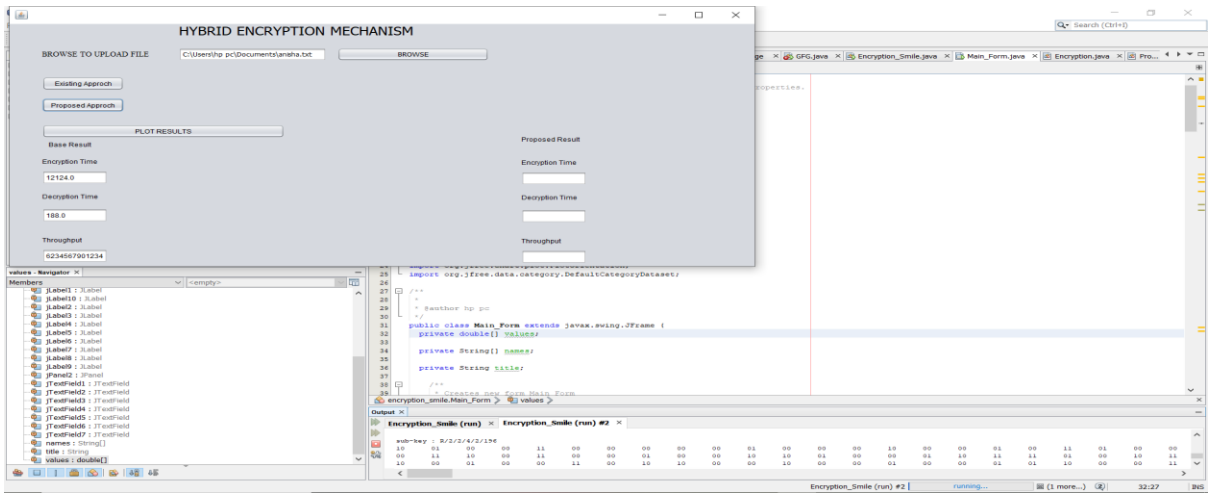

Figure 10: Outcome of proposed approach

Another stage is related to the offline dataset. Kaggle derived this dataset. Both the performance and real time dataset indicates the same outcome.

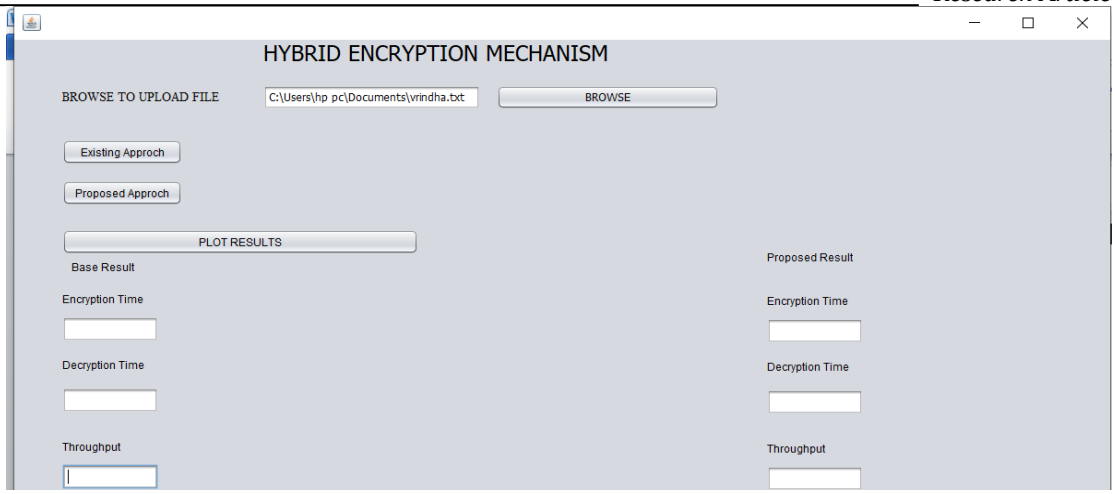

Figure 11: Offline dataset

The outcome is analysed after applying the exiting approach and by loading the dataset. Again the output is established in throughput, encryption time and decryption time.

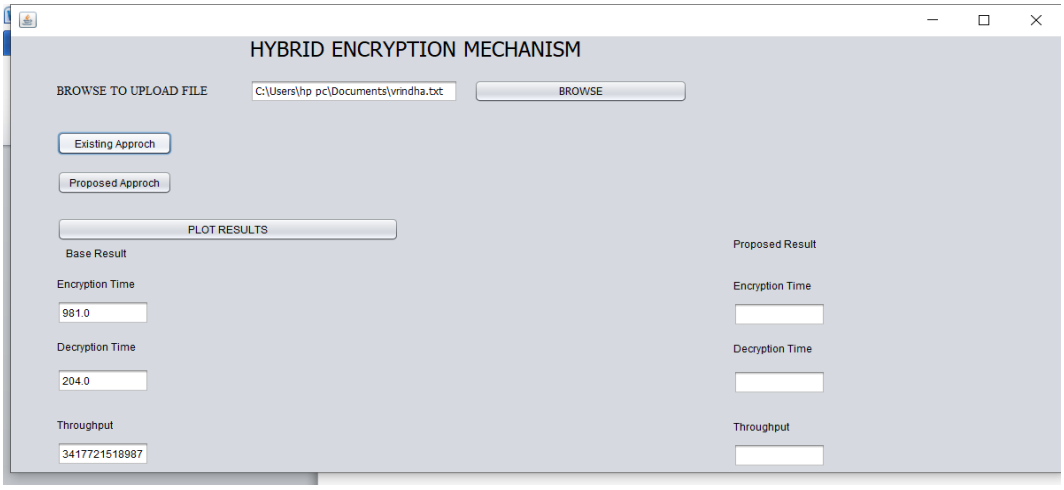

Figure 12:Result of Existing approach

When pressing the proposed button the outcome is acquired that is displayed within the textbox. The obtained outcome is better for the proposed approach.

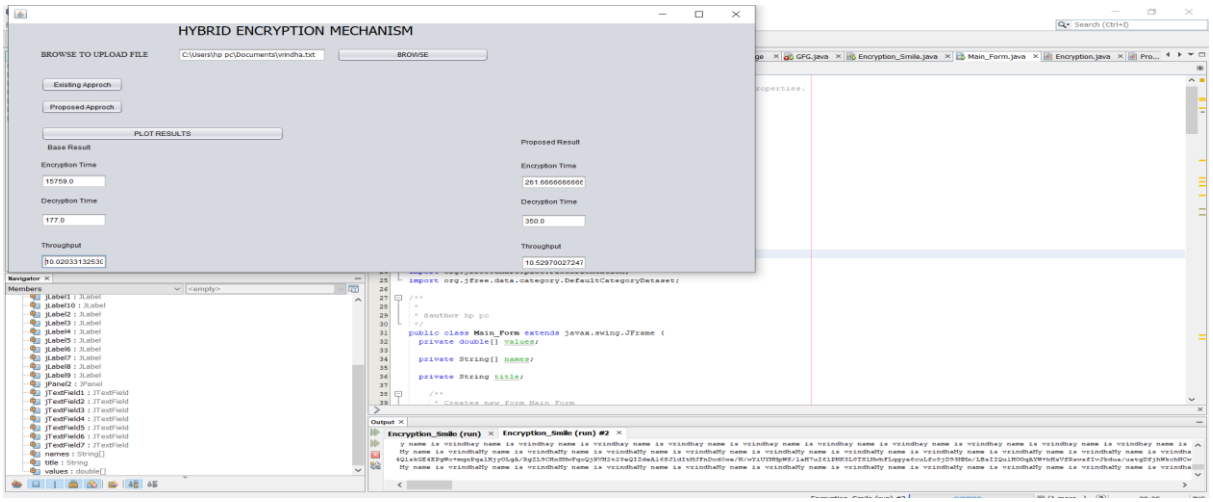

Figure 13: Result of Proposed approach

The result comparison in terms of plots is given in table 6

Parameter	Single tag support	Multiple tag support in block chaining
Encryption Time(ms)	15759	281
Decryption Time(ms)	177	359
Throughput	10.02	10.52

Table 6: Result comparison

The plot for the same is given in figure 14

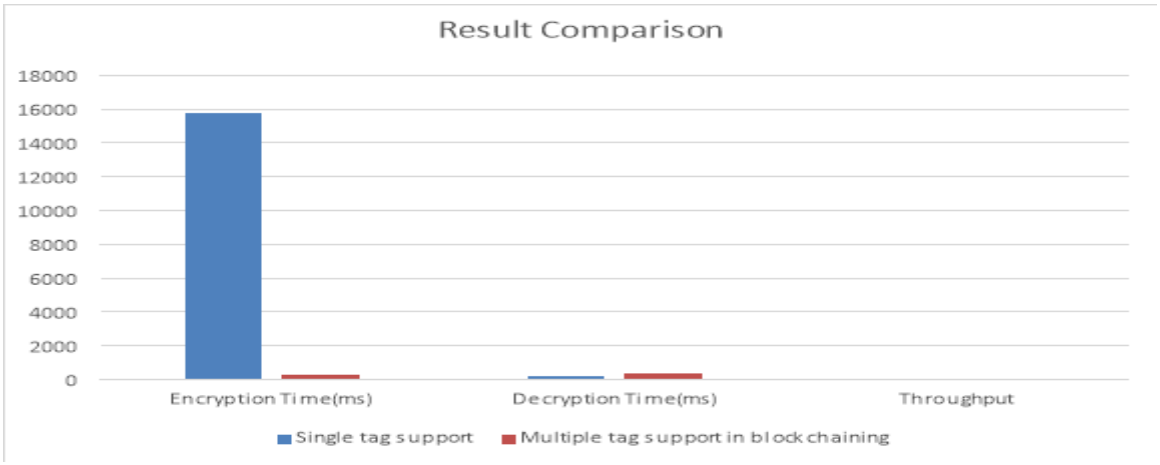

Figure 14: Result Comparison

Discussion of the Findings

In comparison to Block Chaining without Collision detection, the obtained result indicates that purposed approach encryption is much faster. The proposed approach's throughput is increased by minimising data loss, but decryption time is still a significant problem. The explanation for this is that in the event of a collision, data is retrieved from different tag locations. Both real-time and offline datasets produce reliable results, with the offline dataset coming from kaggle.

Conclusion

Banking sector provides improved security through the use of block chaining, which is accompanied by better transactional execution. The collision problem degrades the execution of the block chaining proposal, and the collision problem detection proposal is combined with DNA encryption to handle the collision problem. This means that if a block is created, the key will produce a similar address after a new tag index is added to it, and the similar memory index will be able to hold multiple fields that are linked to the same index. The benefit of achieving encryption time and throughput would be that decryption time decays, causing total execution time to increase. The primary explanation is data retrieval from multiple tag blocks and a collision resolution mechanism. As a result, compressed data can be used in the future against this encryption to reduce decryption time.

References

1. Arora, A. et al. (2017) 'Cloud security ecosystem for data security and privacy', Proceedings of the 7th International Conference Confluence 2017 on Cloud Computing, Data Science and Engineering, pp. 288–292. doi: 10.1109/CONFLUENCE.2017.7943164.
2. Beeputh, A. K., Doomun, M. R. and Dookee, P. (2010) 'Energy-security adaptation scheme of block cipher mode of operations', in Innovations and Advances in Computer Sciences and Engineering, pp. 73–78. doi: 10.1007/978-90-481-3658-2_13.
3. Guo, Y. and Liang, C. (2016) 'Blockchain application and outlook in the banking industry', Financial Innovation. Financial Innovation, 2(1). doi: 10.1186/s40854-016-0034-9.
4. Hu, Y. et al. (2019) 'A Delay-Tolerant payment scheme based on the ethereum blockchain', IEEE Access. IEEE, 7, pp. 33159–33172. doi: 10.1109/ACCESS.2019.2903271.
5. KPMG (2019) 'Blockchain in Finance - KPMG United Kingdom', Website. Available at: https://home.kpmg/uk/en/home/insights/2019/03/bffb-blockchain-in-finance.html (Accessed: 3 January 2021).

6. Li, Y. (2019) 'Emerging blockchain-based applications and techniques', Service Oriented Computing and Applications. Springer London, 13(4), pp. 279–285. doi: 10.1007/s11761-019-00281-x.

7. Malik, M., Singh, A. P. and Narain, P. (2017) 'To Enhance the Data Security of Cloud in Cloud Computing Using Rsa Algorithm', IEEE Access, 3(7), pp. 8–11.

8. Rega, F. G. et al. (2018) 'Blockchain in the banking industry: an Overview The bank of the future, the future of banking View project Blockchain in the banking industry: an Overview', ResearchGate, (September). doi: 10.13140/RG.2.2.25542.32328.

9. Sahi, A., Lai, D. and Li, Y. (2018) 'An Efficient Hash Based Parallel Block Cipher Mode of Operation', in 2018 3rd International Conference on Computer and Communication Systems, ICCCS 2018. Institute of Electrical and Electronics Engineers Inc., pp. 212–216. doi: 10.1109/CCOMS.2018.8463342.

10. Sivanathan, A. et al. (2016) 'Low-Cost Flow-Based Security Solutions for Smart-Home IoT Devices', 10th IEEE International Conference on Advanced Networks and Telecommunications Systems. doi: 10.1109/ANTS.2016.7947781.

11. Stallings, W. (2010) 'NIST block cipher modes of operation for confidentiality', Cryptologia, 34(2), pp. 163–175. doi: 10.1080/01611190903185401.

12. Tsai, W. T. et al. (2017) 'Blockchain Application Development Techniques', Ruan Jian Xue Bao/Journal of Software. Chinese Academy of Sciences, 28(6), pp. 1474–1487. doi: 10.13328/j.cnki.jos.005232.