Research Article

Design and Evaluation to Calculate the Performance of Hybrid Cryptography to make Secure Transaction over Network

Anup Bhange[1] & Dr. Harsh Mathur[2]
[1]PhD Scholar, Department of CSE, Madhyanchal Professional University, Bhopal
[2]Associate Professor, Department of CSE Madhyanchal Professional University, Bhopal

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: Nowadays, the use of internet are growing increasingly across the world, security becomes a prime concern of issue for the society. Earlier security was a major issue for military applications but now the area of applications has been enhanced since most of the communication takes place over the web. Cryptography is an area of computer science which is developed to provide security for the senders and receivers to transmit and receive confidential data through an insecure channel by a means of process called Encryption/ Decryption.

Cryptography might be a model to secure network and knowledge adjoin network. Info Safety is that the required Feature of protective knowledge, Transmission over unsecured network. Cryptography might be a way of loading and forwarding info during a much secured approach so as that solely receiver will scan and work thereon.

In this we paper we emphasis on the matter facing while performing the transaction online i.e transaction failure, attack etc. for that we recommend a replacement hybrid cryptographic process in paper. The algorithm is taken into account using grouping of two cryptographic algorithms Blowfish and RSA. Then Analyze and compare the performance of current and planned algorithm on parameters security, encryption time, and decryption time and message size.

In this research work we made Android application by using Android Studio used for front and for rear for storing the info used PhP My Admin. Results shows the enactment of Hybrid model improved than current procedure.

Key words: Hybrid Cryptography, Blowfish and RSA Algorithm.

1. Introduction

In this period, everything is web focused. Presently every one of the world uses web for appropriation the information. The sent information should be gotten from the vindictive clients. For getting this information, Cryptography is that the best regularly utilized security method. Cryptography is that the techniques for safe dispatch and practice. Its show of adjusting Human comprehensible information into Unreadable structure.

It is isolated in to 2 kinds. 1. Symmetric and Asymmetric key Cryptography. In same private keys utilized for similarly encoding and interpreting takings home by consuming shared mystery key. In awry key cryptosystem the deciphering and encoding customs disparate keys for example Private Key's utilized for interpreting and public keys reused for encoding.

Basic Terms Used in Cryptography

Plain Text The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send “Hello Friend how are you” message to the person Bob. Here “Hello Friend how are you” is a plain text message.

Cipher Text the message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example,

“Ajd672#@91ukl8*^5%” is a Cipher Text produced.

Encryptiona process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

Decryptiona reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

Key: A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "President" then Cipher Text produced will be "Suhvlghqw".

Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

Confidentiality Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

Authentication The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

Integrity Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Non Repudiation ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

Access Control only the authorized parties are able to access the given information.

2. Literature Survey

Symmetric and Asymmetric Cryptographic Algorithm Associated Work

In [1] Study existing the show the blowfish methodology with whole time involved for encoding, slide result and sum from various testing circumstances. The Blowfish methodology was utilized on FPGA utilizing VHDL language. The results introduced that dropping the rounds of Feistel decline all out encoding period, gave better material and not trouble avalanche result interestingly.

In [2], Researchers inspected the overall covert key strategies checking DES, 3DES, AES, Blowfish. Their execution and productivity was related by encoding changing fillings and degrees. The techniques were executed on two assorted equipment stages to relate their productivity. Toward the end, the outcomes were open which concluded that the Blowfish was the firmest technique.

In [3] the encoding measures in particular DES, AES and BLOWFISH were used for proficiency evaluation in paper. Providing for input size of text records and new outcome, it had been conc1uded that Blowfish strategy chugs less execution time and recognition custom. Blowfish accomplishes around multiple times speedier than AES a few times quicker than DES.

It utilizes less recognition compared with AES and DES. However, AES introduced lamentable productivity meanings compared to extra systems, in the interim it needs extra regulation control. it had been not just firmest by and by likewise brings the great asylum completed tough key size which permits it to be reused in various solicitations like really Encoding; online Safety and Packet Encoding.

In [4], creators examined the altered strategy for RSA with improved security. The wellbeing perspective here was the prohibition of n from the first RSA methodology. In its place, the as of late created spare for n can be reused in similarly the keys. The RSA calculation was probably going to determined factorization sessions.

In [5], paper examined the information figuring method connecting to the cloud data stacking approaches and wellbeing in mimicked circumstance. Journalists reachable a method for conveying data stacking and security in distributed computing burning-through open key cryptosystem RSA.

3. Cryptographic Algorithms

RSA

The RSA is that the asymmetric cryptosystem in commonsense. It's the essential strategy that gives e-example and encoding. In RSA, the degree of assurance is made on the 2 indivisible number's logical computation. During This uneven key strategy distinctive key's utilized for the encryption decoding.

The encoding key's public and subsequently the unraveling key leftovers clandestine. It's certainly hard to find out the exact information from key sign. Really encoding and interpreting measures are accomplished at a muddled expediency when RSA alludes encoded keys of public key cryptography. It's anything but a method which is safeguarded from the beast power session.

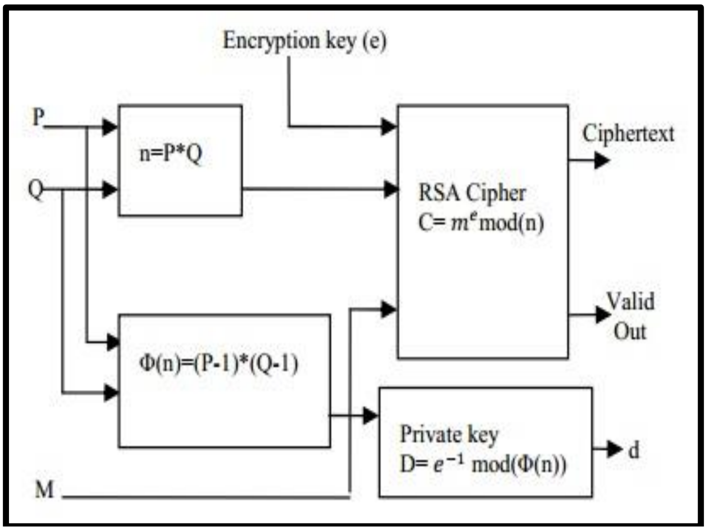


Figure 1: Block Diagram of RSA Algorithm.

Blowfish

Blowfish is block Cipher encoding system based on Feistel reason which customs a 64 cycle square and key size arrangement from 32-448 pieces. It accomplishes 16 rounds. Key development and encoding are the 2 primary part to perform by this technique. Replacement boxes are self-governing of the privileged insights. It requires some investment because of variety of key length. The time extreme sub-key companion measure floods the trouble for an animal power session. It conveys broadened spell data wellbeing with none known secondary passage vulnerability.

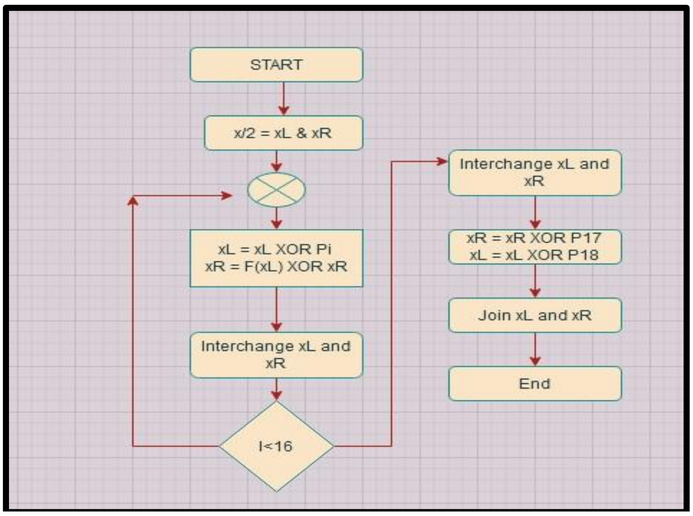


Figure 2: Blowfish Encryption Process.

4. Hybrid Cryptosystem

It is how of encoding that bonds double or extra procedure methods and a mixture of equally asymmetric and symmetric key cryptosystem also comprised. It assistances to use the advantage of equally schemes. The problem of symmetric key procedure is distribution the security keys beforehand and thus the difficult of asymmetric key procedure is calculation. By joining these two procedure helps we to decrease the difficulties confronted in both systems. This hybrid cryptography delivers a far improved security for public keys and thus the general public key cryptosystem rapidity is amplified.

Advantage

- There's no necessity of distribution the key
- Speediness of encoding and decoding surges similar symmetric key cryptosystem
- e-pattern is conceivable since the Keys are sending by RSA
- Improved safety than modest cryptosystem.

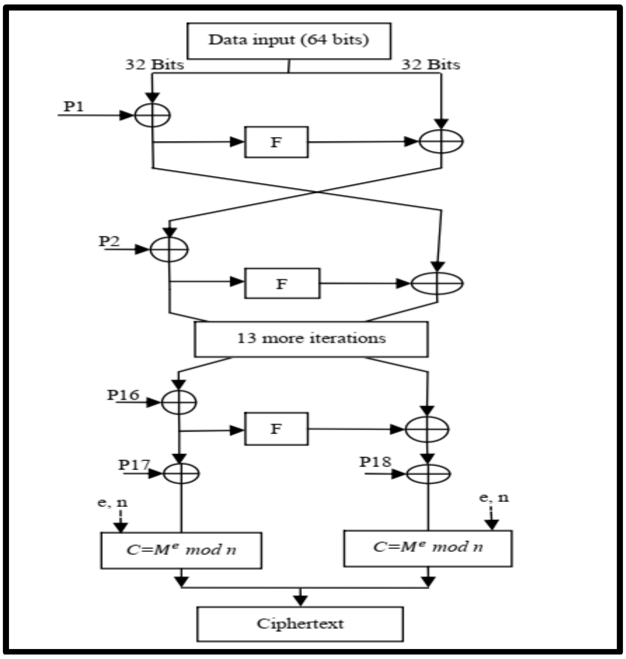


Figure 3: Hybrid Encryption Process.

The Hybrid procedure utilized similarly symmetric and uneven techniques. Subsequently, key benefits of the two strategies are reachable with this arranged examine strategy.

The symmetric strategy is firm responsive, secured, less memory utilized and Straight forward in idea method. The Asymmetric key technique is also notable as open key cryptography. It's generally estimated for Confirmation measure. The unbalanced methodologies are encoded by open key yet decoded by just the legitimate client who has the private key. The focal trouble is that key size fundamental be kept exceptional, so that, it can't be utilized by direct key replacement.

It denotes the strategy to gentler. Yet, this blend framework allows the use of minimal key for unbalanced technique in the meantime straight replacement doesn't exertion since it is aggregate interaction with Blowfish along these lines, the speed of methodology is to quicker than the unmistakable cycle.

The Blowfish is furthermore gets more secure since it needs similarly RSA and blowfish keys for disentangling. Thus, the rounds of blowfish are frequently additionally condensed to eight rounds or 4 rounds which winds up in better speed than prior systems.

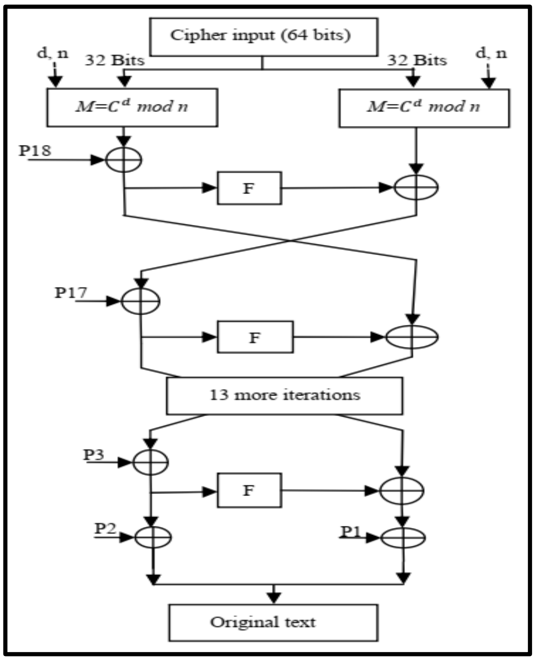


Figure 4: Hybrid Decryption Process.

The decoding system is equal because the encoding, but the P-array is used in other way. The RSA encoding is used impartial next the coded input data. The private key d is to tend here for RSA which is a confirmation key also the encoding and decoding procedures use similar kind of Feistel network. This technique also delivers safety after brute force too. As, dual dissimilar encoding procedures are recycled here, the proper mixture of equally keys is vital to decoded the data which is extremely problematic to understand. So, the planned hybrid method delivers safety and structures healthier than the preceding distinctly recycled approaches. Blowfish and RSA are also influence competent procedures.

Topmost 5 Security Threats Fronting e-Commerce Today

- Distributed Denial of Service (DDoS) Attacks
- Credit card fraud
- Malware.
- Bad bots.
- E-skimming.

So our main approach to focus such issue and develop the model that overcome current threats facing e- commerce today. By using the Hybrid cryptography we are trying to overcome many attacks and above mentioned issue.

5. Proposed Method

To understand the performance of any cryptographic algorithm, first we understand the nature of algorithm, then size, throughput, Encryption and Decryption time and processing time to computer the overall performance of the system.

In our Research work we are going to use the hybrid Cryptosystem i.e Symmetric and Asymmetric.

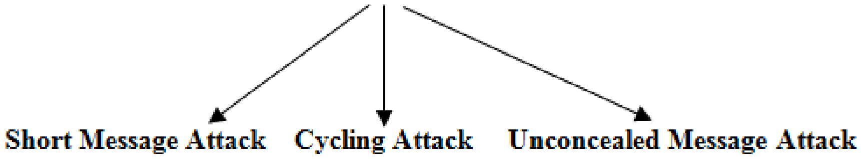
- For Symmetric we use Blowfish Algorithm
- For Asymmetric we use RSA Algorithm

Key Factors of Blowfish

►Key size:- 32 bit to 448bit
►Message size block: 64 bit
►Encryption Round 16
►Sub key generated: 18 for Encryption / Decryption
►It used to prevent the application from guessing attack.
► IT used to prevent Brute force attack.

Key Factors of RSA

►It is slow but provide High Security
►High processing required at Receiver end
►It can prevent from some known attack: Plaintext attack



►Prevent from Factorization **attack**
►**Key size:** 1024, 2048, or 4096 bit
►**Encryption Process**
Step-1: Choose dual prime number p and q
Step-2: Calculate the value of n and Ǿ
Step-3: Find the value of e (public key)
Step-4: Compute the value of d (private key)
Step-5: Do the encryption and decryption

In our work we see that the response time, Encryption and Decryption time from server depends on the various parameter. As we see that many account number length varies from bank to bank as per the RBI. The following are guidelines from the RBI.

- Account number length varies since 9 digits to 18 digits.
- Most of the banks (67 out of 78) have included branch code as part of the account number structure. Some banks have product code as part of the account number structure.
- 40 out of 78 banks do not have check digit as part of the account number structure.

So we are getting some observation if we insert the short length data, it required less time for encryption and decryption (also depends on network speed, Processor speed also) means faster response get less chance of attack.

https://www.psubankers.in/2019/04/No-of-Digits-in-Account-Number-of-Different-Banks-in-India.html ***(link to see the size of account no of banks)***

In proposed algorithm (Hybrid Blowfish and RSA) the objective had been accomplished by merging two algorithms called Blowfish and RSA. Fig 2 depicts the work flow process of our hybrid algorithm.

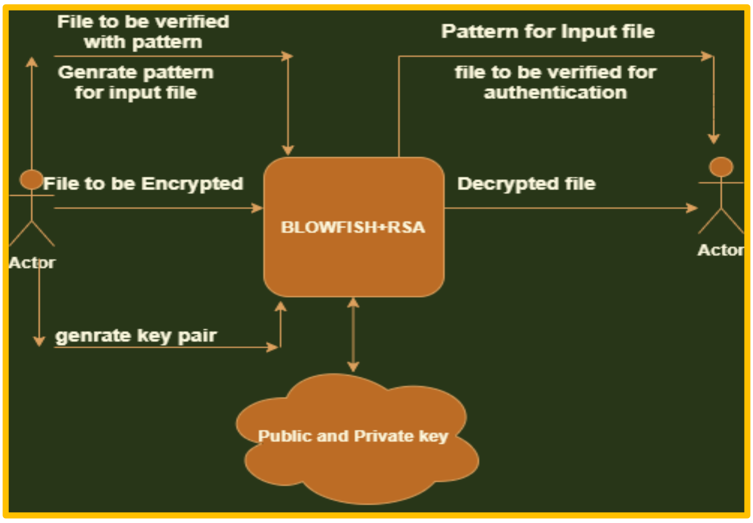


Figure 5: Work Flow Process of BLOWFISH+RSA.

6. Experimental Setup

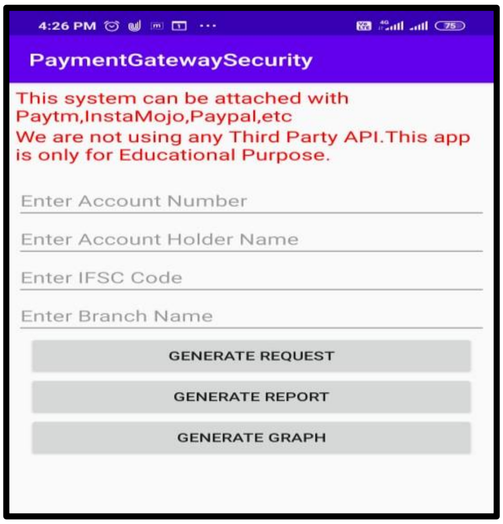
Android Studio

Android Studio is the authorized combined progress situation for Google's Android operating system, constructed on Jet Brains' IntelliJ IDEA software and intended precisely for Android expansion.

PhpMyAdmin

Php My Admin is a free and open supply
Administration tool for MySQL.

Home Page of Application



PaymentGatewaySecurity

This system can be attached with Paytm,InstaMojo,Paypal,etc
We are not using any Third Party API.This app is only for Educational Purpose.

Enter Account Number

Enter Account Holder Name

Enter IFSC Code

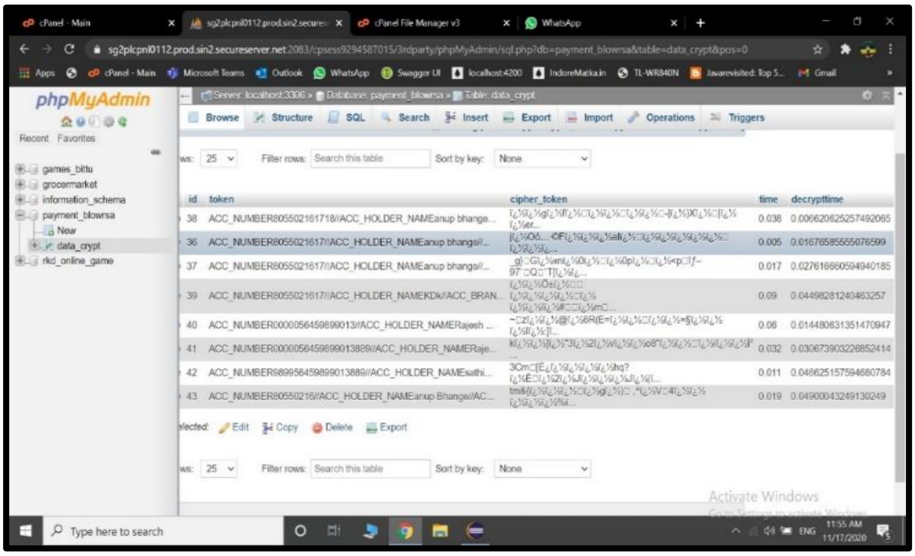
Enter Branch Name

Figure 6: Home Page of Application.

Following Process to be Considered while Use above Application

1. As we mentioned that we are prepared the Application to carry out our research work. As we said that we used the hybrid cryptography technique to secure payment gateway.
2. After opening the application we have to fill some mandatory information i.e ACC NO, NAME, IFSC CODE, BRANCH NAME then clique on the generate request and Then all the data should be stored at backend that is Php admin.
3. Here some noticeable point is that encryption and decryption time, Performance, id, token generated and it depends on the size of message and algorithm.
4. After submitting the all the details, now we have click on generate report. Its will shows the time required for the encryption and decryption.
5. As result it first generate the token then achieve the encoding and decoding process also shows the time for encryption and decryption.
6. After that we compare the result

7. Database Screen Shot



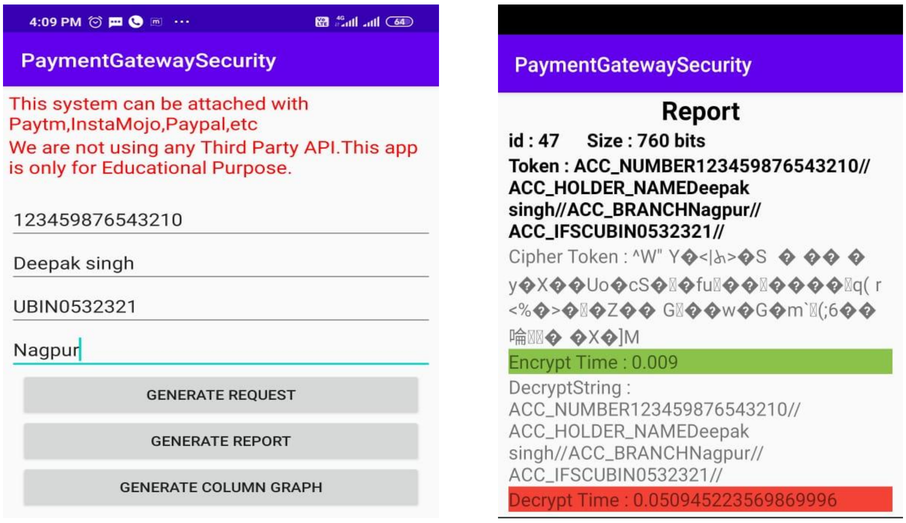
Server: localhost:3306 » Database: payment_blowrsa » Table: data_crypt

id	token	cipher_token	time	decrypttime
38	ACC_NUMBER805502161718//ACC_HOLDER_NAMEanup bhange...	ï¿½ï¿½gï¿½fï¿½□ï¿½ï¿½□ï¿½ï¿½□-[ï¿½)Xï¿½□[ï¿½ ï¿½er...	0.038	0.006620625257492065
36	ACC_NUMBER8055021617//ACC_HOLDER_NAMEanup bhange//...	jï¿½Oô...©Fï¿½ï¿½ï¿½allï¿½□ï¿½ï¿½ï¿½ï¿½ï¿½□ ï¿½ï¿½...	0.005	0.01676585555076599
37	ACC_NUMBER8055021617//ACC_HOLDER_NAMEanup bhange//...	_g)□Gï¿½xmï¿½0ï¿½□ï¿½0pï¿½□ï¿½<p□f~ 97□Q□'T[ï¿½...	0.017	0.027616660594940185
39	ACC_NUMBER8055021617//ACC_HOLDER_NAMEKDk//ACC_BRAN...	ï¿½ï¿½Oï¿½□□ ï¿½ï¿½ï¿½□ï¿½ ï¿½ï¿½ï¿½#□□ï¿½m□...	0.09	0.04498281240463257
40	ACC_NUMBER0000056459899013//ACC_HOLDER_NAMERajesh ...	~□zï¿½ï¿½@ï¿½6R(E=ï¿½ï¿½□ï¿½ï¿½×§ï¿½ï¿½ ï¿½ï¿½]...	0.06	0.014480631351470947
41	ACC_NUMBER0000056459899013889//ACC_HOLDER_NAMERaje...	kï¿½ï¿½]ï¿½*3ï¿½2ï¿½ï¿½ï¿½o8"ï¿½ï¿½□ï¿½ï¿½ï¿½P ...	0.032	0.030673903226852414
42	ACC_NUMBER989956459899013889//ACC_HOLDER_NAMEsathi...	3Cm□[Eï¿½ï¿½ï¿½ï¿½hq? ï¿½Ë□ï¿½2ï¿½Jï¿½ï¿½ï¿½Jï¿½[...	0.011	0.046625157594680784
43	ACC_NUMBER80550216//ACC_HOLDER_NAMEanup Bhange//AC...	tm&[ï¿½ï¿½ï¿½□ï¿½gï¿½)□ .^ï¿½V□4ï¿½ï¿½ ï¿½ï¿½ï¿½%i...	0.019	0.04900043249130249

Figure 7: Database Screen Shot.

8. Report Generation for Application-1

Here we are considering the example for Union bank account no here the length of account no is 15 digit.



This system can be attached with Paytm,InstaMojo,Paypal,etc
We are not using any Third Party API.This app is only for Educational Purpose.

123459876543210

Deepak singh

UBIN0532321

Nagpur

GENERATE REQUEST

GENERATE REPORT

GENERATE COLUMN GRAPH

Report

id : 47 Size : 760 bits

Token : ACC_NUMBER123459876543210// ACC_HOLDER_NAMEDeepak singh//ACC_BRANCHNagpur// ACC_IFSCUBIN0532321//

Cipher Token : ^W" Y�<|ꝏ>�S � �� � y�X��Uo�cS��fu���������q(r <%�>��Z�� G��w�G�m`(;6�� 喻� �X�]M

Encrypt Time : 0.009

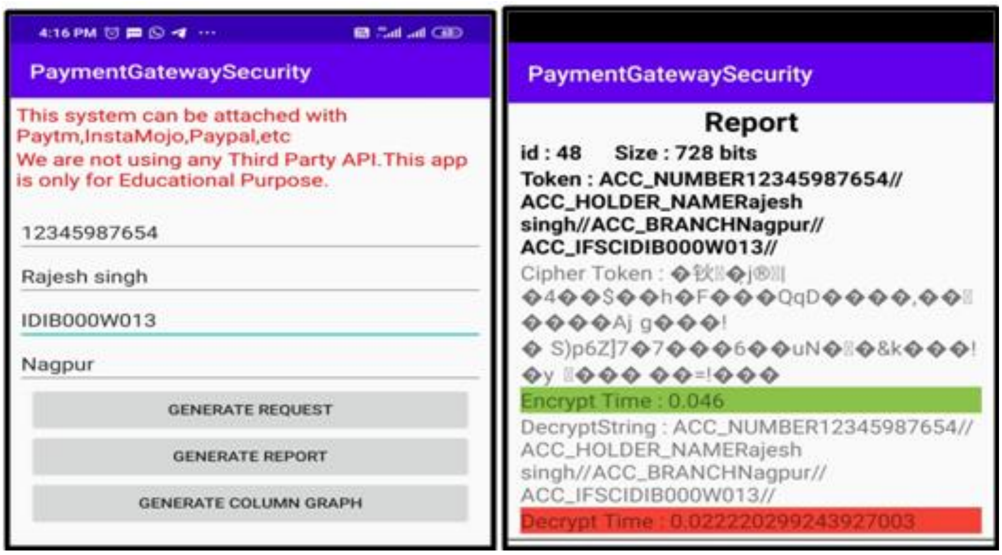
DecryptString : ACC_NUMBER123459876543210// ACC_HOLDER_NAMEDeepak singh//ACC_BRANCHNagpur// ACC_IFSCUBIN0532321//

Decrypt Time : 0.050945223569869996

Figure 8: Report Generation-1.

This is the report for above mentioned message it shows the id, bits size, encryption and decryption time required to computer the message.

Report Generation for Application-2



This system can be attached with Paytm,InstaMojo,Paypal,etc
We are not using any Third Party API.This app is only for Educational Purpose.

12345987654

Rajesh singh

IDIB000W013

Nagpur

Report

id : 48 Size : 728 bits

Token : ACC_NUMBER12345987654//ACC_HOLDER_NAMERajesh singh//ACC_BRANCHNagpur//ACC_IFSCIDIB000W013//

Cipher Token : �钬�j®
�4��$��h�F���QqD����,��
����Aj g���!
� S)p6Z]7�7���6��uN��&k���!
�y ��� ��=!���

Encrypt Time : 0.046

DecryptString : ACC_NUMBER12345987654//ACC_HOLDER_NAMERajesh singh//ACC_BRANCHNagpur//ACC_IFSCIDIB000W013//

Decrypt Time : 0.022220299243927003

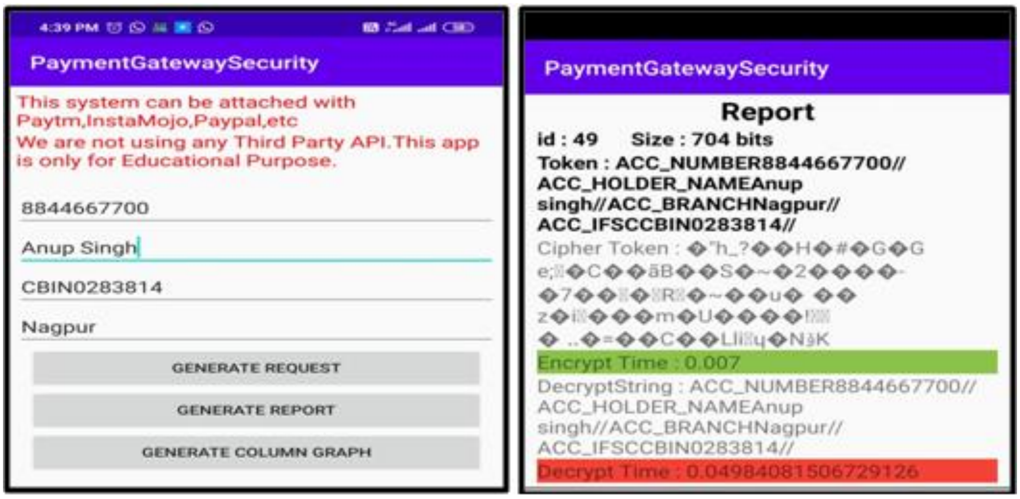
Figure 9: Report Generation-2.

Here we are considering the example for Indian bank account no here the length of account no is 11 digit. So here we see that when we compare to above result with above data it take less time decryption. So it concludes that the encryption and decryption time also depends on the size of bits. Bit size means less time for encryption and more time for decryption.

In second observation we see that the message is less but it take more time for encryption but less time for decryption means received the faster response from server (i.e depends on processor, network speed)

Report Generation for Application-3

Here we are considering the example for Indian bank account no here the length of account no is 10 digit. As we mentioned above time required for encryption and decryption depends on size and algorithm and network speed also. Here we found that due to network issue we got conflict result. Here time taken for decryption is more compare to encryption. It Satisfy our first condition less bits data i.e. less time for Encryption but due to network issue it take more time decryption.



This system can be attached with Paytm,InstaMojo,Paypal,etc
We are not using any Third Party API.This app is only for Educational Purpose.

8844667700

Anup Singh

CBIN0283814

Nagpur

Report

id : 49 Size : 704 bits

Token : ACC_NUMBER8844667700//ACC_HOLDER_NAMEAnup singh//ACC_BRANCHNagpur//ACC_IFSCCBIN0283814//

Cipher Token : �"h_?��H�#�G�G
e;�C��ãB��S�~�2����-
�7����R�~��u� ��
z�i���m�U����!
� ..�=��C��Lli�y�NȝK

Encrypt Time : 0.007

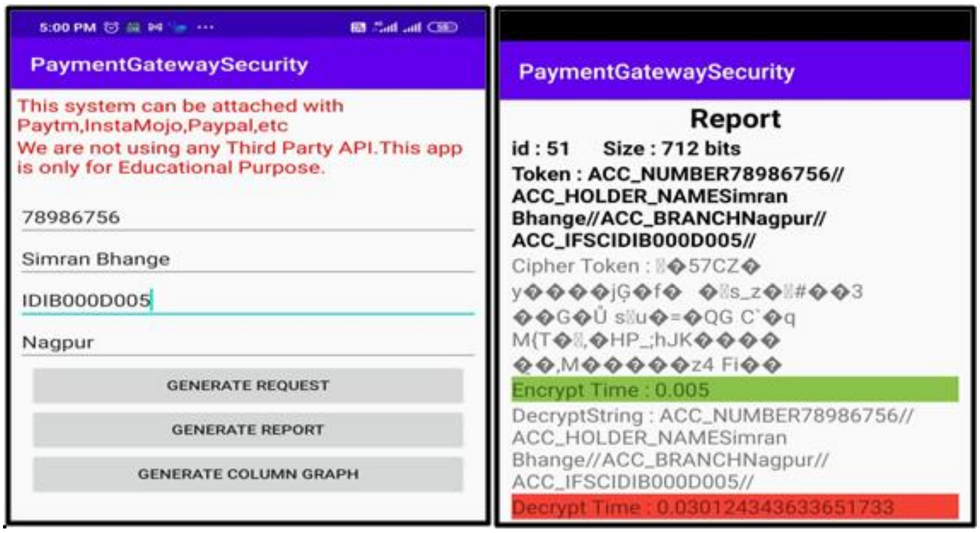
DecryptString : ACC_NUMBER8844667700//ACC_HOLDER_NAMEAnup singh//ACC_BRANCHNagpur//ACC_IFSCCBIN0283814//

Decrypt Time : 0.04984081506729126

Figure 10: Report Generation-3.

Report Generation for Application-4

Here we are considering the example for Indian bank account no here the length of account no is 09 digit. So here we see that when we compare to above result with above data it take less time decryption. So it concludes that the encryption and decryption time depends on the size of bits. Bit size less means less time for encryption and more time for decryption. In second observation we see that the message is less but it take more time for encryption but less time for decryption



This system can be attached with Paytm,InstaMojo,Paypal,etc
We are not using any Third Party API.This app is only for Educational Purpose.

78986756

Simran Bhange

IDIB000D005

Nagpur

Report

id : 51 Size : 712 bits

Token : ACC_NUMBER78986756//ACC_HOLDER_NAMESimran Bhange//ACC_BRANCHNagpur//ACC_IFSCIDIB000D005//

Cipher Token : ▯�57CZ�y����jĢ�f� �▯s_z�▯#��3��G�Ů s▯u�=�QG C`�qM(T�▯,�HP_;hJK������,M������z4 Fi��

Encrypt Time : 0.005

DecryptString : ACC_NUMBER78986756//ACC_HOLDER_NAMESimran Bhange//ACC_BRANCHNagpur//ACC_IFSCIDIB000D005//

Decrypt Time : 0.030124343633651733

Figure 11: Report Generation-4.

9. Result Analysis of Proposed Hybrid System

Table 1: Result Analysis

Proposed Algorithm	Id	Message Size	Encryption Time	Decryption Time
Blowfish+RSA	47	750 bits	0.009	0.05
	48	735 bits	0.046	0.022
	49	710bits	0.013	0.05
	51	715 Bits	0.005	0.03

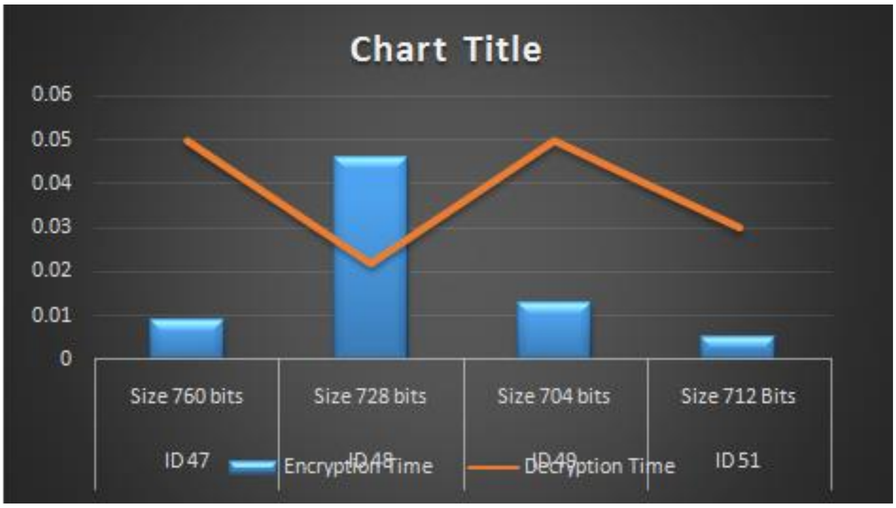


Figure 12: Result Analysis of Proposed Hybrid System.

Existing Available Data Using Hybrid System

Table 2: Existing Available Data using Hybrid System

	Encryption						Decryption		
Size	**512-bit**	**Size**	**1024-bit**	**Size**	**2048-bit**	**Size**	**512-bit**	**1024-bit**	**2048-bit**
1 KB	0.218	2.88	0.171	2.88	0.328	3	1.872	7.504	24.461
2 KB	0.39	5.69	0.343	5.75	0.562	5.75	3.869	13.51	45.75
3 KB	0.406	8.5	0.484	8.5	1.014	8.5	5.039	20.764	67.938
4 KB	0.421	11.3	0.546	11.3	1.264	11.5	6.63	24.772	90.09
5 KB	0.468	14.1	0.593	14.1	1.326	14.2	8.19	31.309	110.698
6 KB	0.499	16.9	0.702	17	1.342	17	11.076	37.752	156.032
7 KB	0.546	19.7	0.874	19.7	1.529	19.7	16.349	48.243	188.527
8 KB	0.562	22.5	0.999	22.6	1.716	22.6	18.564	57.842	197.744
9 KB	0.702	25.3	1.154	25.3	1.732	25.3	19.203	64.774	205.157
10 KB	0.733	28.1	1.248	28.2	1.872	28.2	20.885	72.252	218.168

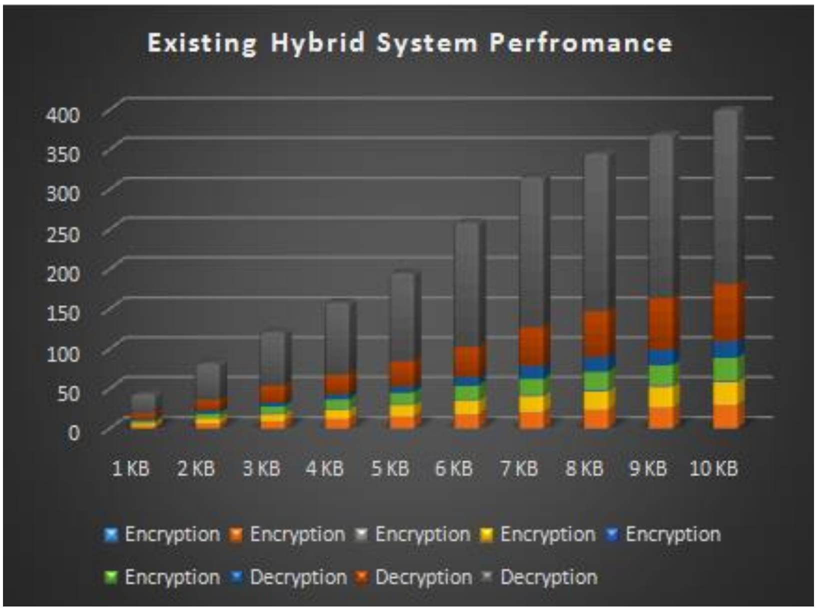


Figure 13: Result Analysis of Existing Hybrid System.

10. Conclusions

Many algorithms has been developed to satisfy the security goals which are integrity, confidentiality, non-reputation and authentication. These encryption algorithms can easily be chosen according to the data type which actually being communicated and the channel type which used for communicate the data.

As compare with the proposed work, the existing system performance is poor in terms of Encryption, Decryption time, message size. Our proposed system give better result because we took universal message size, our system automatically calculate the size of message and existing system consider the very low size of bits. As well as it take more time to encrypt the message. So the performance of any system is depends on the following parameter. 1. Processor 2. Key size. 3. Encryption time 4. Decryption time 5. Response from server.

References

1. Nadeem, A.; Javed, M.Y., "A performance comparison of data encryption algorithms," International Conference on Information and Communication Technologies, vol. no. 1, pp.84-89, 27-28 Aug. 2005.
2. Ramesh, A.; Suruliandi, A., "Performance analysis of encryption algorithms for Information Security," International Conference on Circuits, Power and Computing Technologies, vol., no. 2, pp.840-844,20-21 March 2013.
3. Prasetyo, K.N.; Purwanto, Y.; Darlis, D., "An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA, "International Conference on Information and Communication Technology, vol., no. 2, pp.75-79, 28-30 May 2014

4. Minni, R.; Sultania, K.; Mishra, S.; Vincent, D.R., "An algorithm to enhance security in RSA," International Conference on Computing, Communications and Networking Technologies, vol., no. 4, pp.1-4, 4-6July 2013.
5. Yellamma, P.; Narasimham, C.; Sreenivas, V., "Data security in cloud using RSA," International Conference on Computing, Communications and Networking Technologies, vol. no. 4, pp.1-6, 4-6 July 2013.
6. AnupBhange, Dr. Harsh Mathur"Comparative Analysis Of Several Cryptography Algorithm With Its Effectiveness Towards The Security And Its Performance" Vol. 21 No. 6 (2019) ISSN SSN: 0374-8588
7. AnupBhange,Dr. Harsh Mathur "Design security structure to secure payment gateway using hybrid cryptography" Journal of Seybold Report Volume 15 Issue 8 August-2020.ISSN 1533-9211
8. Sameer Saxena, Sonali Vyas2, B. Suresh Kumar3, Shaurya Gupta "Survey on Online Electronic Paymentss Security" 978-1-5386-9346-9/19/$31.00 ©2019 IEEE
9. A. Mani Kandan, G. JaspherWillsie Kathrine, Alfred Raja Melvin, "Network Attacks and Prevention techniques – A Study " 978-1-5386-8158-9/19/$31.00©2019IEEE
10. Anup Bhange ,Dr. Harsh Mathur "Performance Evaluation, Analysis and Design of an Innovative Structure to Secure the Payment Gateways using Hybrid Cryptography" Asian Journal of Information Technology ISSN : ISSN: 1682-3915DOI: 10.36478/ajit.2021.33.40