ASIAN JOURNAL OF INFORMATION TECHNOLOGY
MEDWELL PUBLICATIONS

Performance Evaluation, Analysis and Design of an Innovative Structure to Secure the Payment Gateways using Hybrid Cryptography

Anup Bhange and Harsh Mathur
Department of Computer Science and Engineering (CSE), Madhyanchal Professional University (MPU) Bhopal, Madhya Pradesh, India

Key words: Cryptography, Blowfish and RSA algorithm

Corresponding Author:
Anup Bhange
Department of Computer Science and Engineering (CSE), Madhyanchal Professional University (MPU) Bhopal, Madhya Pradesh, India

Page No.: 33-40
Volume: 20, Issue 2, 2021
ISSN: 1682-3915
Asian Journal of Information Technology

Abstract: Cryptography could be a model to secure network and knowledge adjoin network. Info safety is that the necessary feature of protective knowledge transmission over unsecured network. Cryptography could be a technique of loading and forwarding info in a much secured approach in order that solely receiver will scan and work thereon. In this study we emphasis on the problem facing while performing the transaction online, i.e., transaction failure, attack, etc., for that were commend a new hybrid cryptographic process in study. The algorithm is considered using grouping of two cryptographic algorithms Blowfish and RSA. After that Analyze and compare the performance of current and planned algorithm on parameters security, encryption time, decryption time and message size. In this research work, we made Android application by using Android Studio used for front end and for back end for storing the data used php My Admin. Results shows the performance of Hybrid model better than existing algorithm.

INTRODUCTION

In this era, all is web centered. Now, all the world uses web for distribution the data. The transmitted data must be secured from the malevolent customers. For securing this data, Cryptography is that the best frequently used safety technique. Cryptography is that the methods for safe communiqué and rehearsal. It show of altering human readable data into unreadable form.

It is separated in to 2 types. Symmetric and asymmetric key cryptography. In same private keys used for equally encoding and decoding takings residence by expending shared secret key. In asymmetric key crypto system the decoding and encoding customs dissimilar keys, i.e., private key's used for decoding and public key's recycled for encoding.

Literature review

Blowfish algorithm and RSA algorithm related work: By Nadeem and Javed[1] study existing the show the blowfish procedure with entire time occupied for encoding, slide result and amount from numerous challenging situations. The Blowfish procedure was employed on FPGA using VHDL language. The outcomes presented that dropping the rounds of Feistel decrease total encoding period, gave better material and not distress landslide out come suggestively.

By Ramesh and Suruilandi[2], examined the general stealthy key procedures counting DES, 3DES, AES, Blowfish. Their execution and efficiency was associated by encoding changing fillings and extents. The procedures were executed on two diverse hardware stages to associate their efficiency at the end, the results were accessible which decided that the Blowfish was the firmest procedure.

By Prasetyo *et al*.[3] the encoding processes namely DES, AES and BLOWFISH were utilize for efficiency assessment in paper. Giving to input size of text records and new consequence, it had been conc1uded that Blowfish procedure guzzles fewer performance time and remembrance custom. Blowfish achieves around 4 times quicker than AES and a couple of times faster than DES. It uses fewer remembrance likened with AES and DES. Though, AES presented unfortunate efficiency significances likened to additional procedures, meanwhile it needs additional dispensation control it had been not only firmest never the less also brings the good refuge finished sturdy key size which allows it to be recycled in numerous requests like more encoding; web based Safety and Packet Encoding.

By Minni *et al*.[4], researchers discussed the modified procedure for RSA with improved safety. The safety point of view here was the exclusion of n from the original RSA procedure. In its place, the recently produced spare for n can be recycled in equally the keys. The RSA algorithm was likely toto calculated factorization bouts.

By Yallamma[5], study discussed the data figuring technique linking to the cloud information loading approaches and safety in simulated situation. Writers obtainable a technique for delivering information loading and safety in cloud computing consuming public key cryptosystem RSA.

Cryptographic algorithms

RSA: The RSA is that the asymmetric-key cryptosystem in practical. It's the primary procedure that gives e-pattern and encoding. In RSA, the extent of protection is made on the 2 prime number's scientific calculation. During this asymmetric key procedure different key's used for the encryption decryption.

The encoding key's public and therefore the decoding key remainders surreptitious. It's surely tough to ascertain the precise info from key signal. More encoding and decoding processes are achieved at a complicated speediness when RSA refers encoded keys of public key cryptography. It's also an procedure which is shielded from the brute force bout (Fig. 1).

BLOWFISH

Blowfish is block cipher encoding procedure built on Feistel purpose which customs a 64 bit block and key size series from 32-448 bits. It achieves 16 rounds. Key enlargement and encoding are the 2 main part to perform by this procedure. Substitution boxes are autonomous of the secrets. It take more performing time due to variation of key length. The time intense sub-key cohort process surges the difficulty for a brute-force bout. It delivers extended stint information safety with none known backdoor susceptibility (Fig. 2).

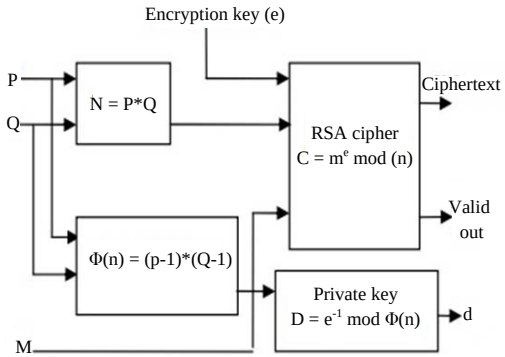

Fig. 1: Block diagram of RSA algorithm

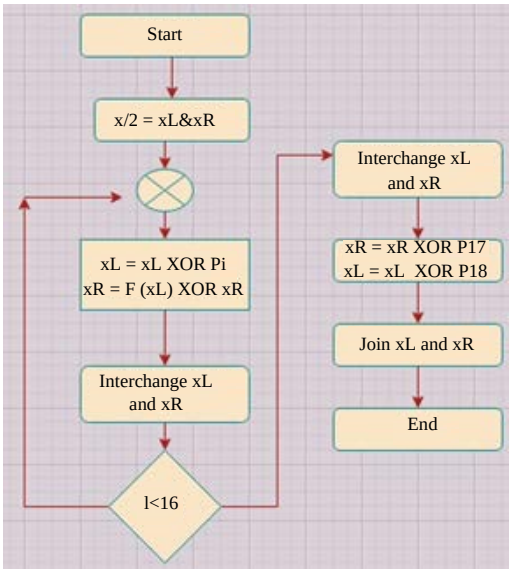

Fig. 2: Blowfish encryption process

Hybrid cryptosystem: It is a way of encoding that bonds double or extra procedure methods and a mix of equally asymmetric and symmetric key cryptosystem also comprised. It assistances to use the benefit of equally schemes. The difficulty of symmetric key procedure is distribution the safety keys beforehand and therefore 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 therefore, the 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

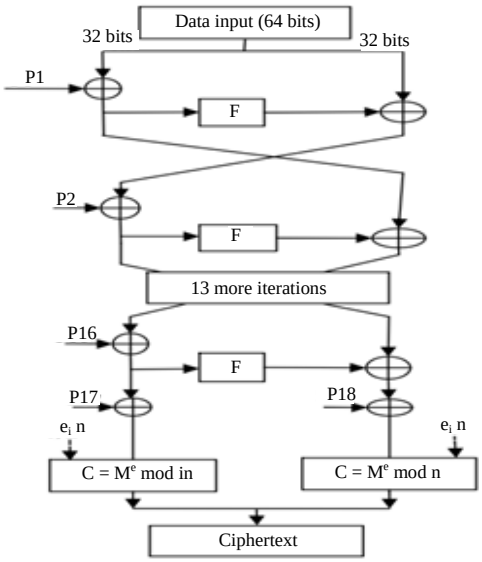

Fig. 3: Hybrid encryption process

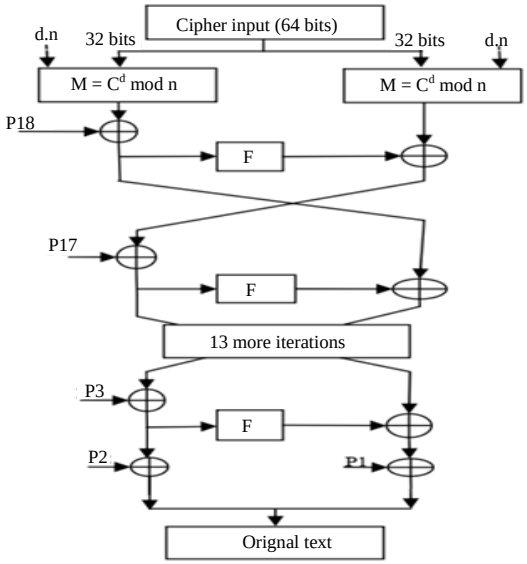

Fig. 4: Hybrid decryption process

- E-pattern is conceivable since the keys are sending by RSA
- Improved safety than modest cryptosystem

The hybrid technique used equally symmetric and asymmetric methods. Thus, key advantage of both methods are reachable with this planned discuss technique (Fig. 3).

The symmetric method is firm responsive, protected, fewer memory used and straightforward in concept technique. The asymmetric method is additionally well-known as public key cryptography. It's mostly measured for confirmation process. The asymmetric approaches are encoded by public key but decrypted by only the valid user who has the private key. The central difficulty is that key size essential be kept extraordinary, so that, it can't be employed by direct key substitution.

It marks the tactic to gentler. But this mix system permits the utilization of little key for asymmetric method mean while straight substitution doesn't effort because it is collective process with Blowfish so, the quickness of procedure is to faster than the distinct process.

The Blowfish is additionally becomes safer, since, it wants equally RSA and blowfish keys for decoding. So, the rounds of blowfish are often also abridged to eight rounds or 4 rounds which ends up in healthier rapidity than earlier procedures (Fig. 4).

The decoding system is equal because the encoding but the P-array is employed in opposite direction. The RSA encoding is employed impartial next the coded input file. The private key d is to tend here for RSA which is an confirmation key also the encoding and decoding procedures use similar sort of Feistel network. This system also delivers safety after brute force too. As, dual dissimilar encoding procedures are recycled here, the right mixture of equally keys is important to decoded the info which is extremely problematic to realize. So, the planned hybrid method delivers safety and structures healthier than the preceding distinctly recycled approaches. Blowfish and RSA also are 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.

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 448 bit
- 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

Short message attack cycling attack Unconcealed message 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
    - 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 research, 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.

About 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. Figure 2 depicts the work flow process of our hybrid algorithm (Fig. 5).

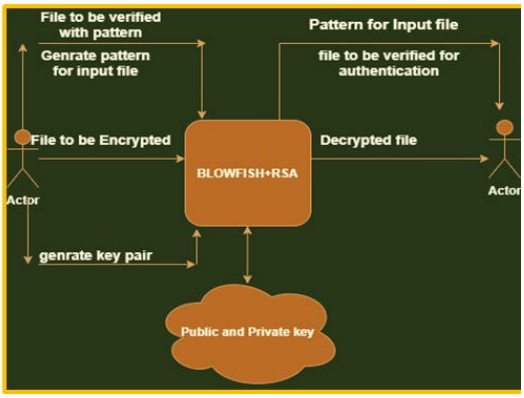

Fig. 5: Work flow process of Blowfish+RSA

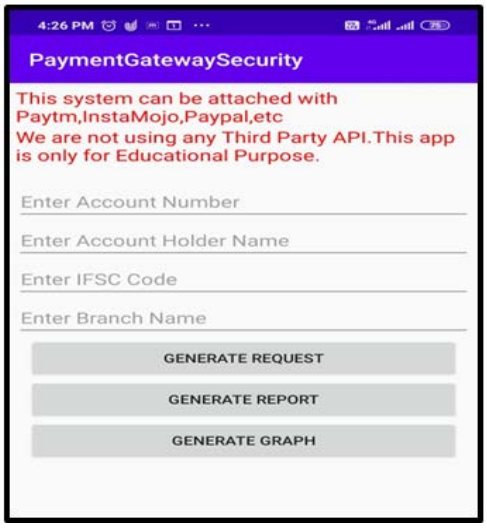

Fig. 6: Home page of application

EXPERIMENTAL SETUP

Android studio: Android Studio is the authorized combined progress situation for Google's Android operating system, constructed on Jet Brain's Intelli J IDEA Software and intended precisely for Android expansion Php My Admin. Php My Admin is a free and open supply administration tool for MySQL (Fig. 6).

Home page of application: Following process to be considered while use above application: 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.

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.

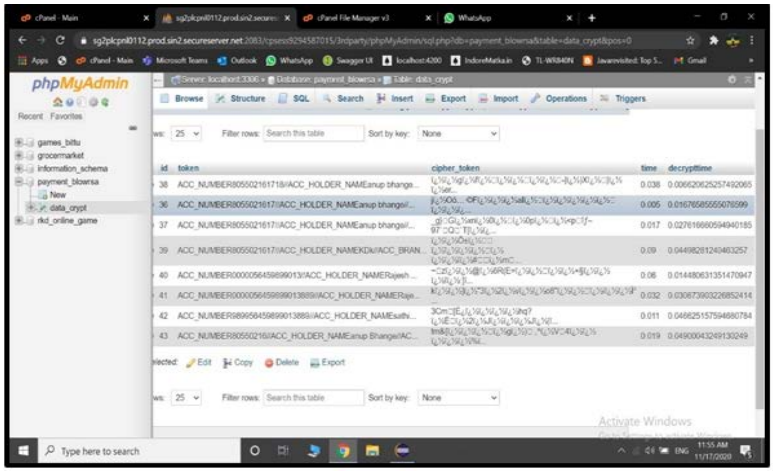

Fig. 7: Database screen shot

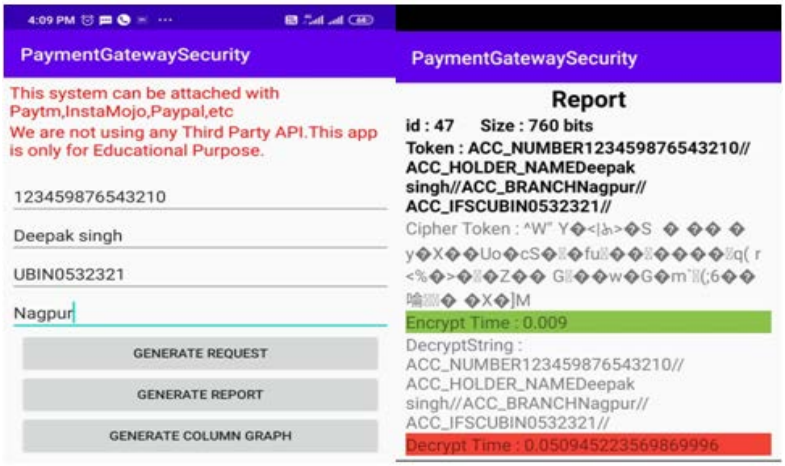

Fig. 8: Report generation

Here, some noticeable point is that encryption and decryption time, performance, id, token generated and it depends on the size of message and algorithm.

After submitting the all the details, now we have click on generate report. Its will shows the time required for the encryption and decryption. As result it first generate the token then achieve the encoding and decoding process also shows the time for encryption and decryption. After that we compare the result (Fig. 7)

Database screen shot

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 (Fig. 8).

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: 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 (Fig. 9 and 10).

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

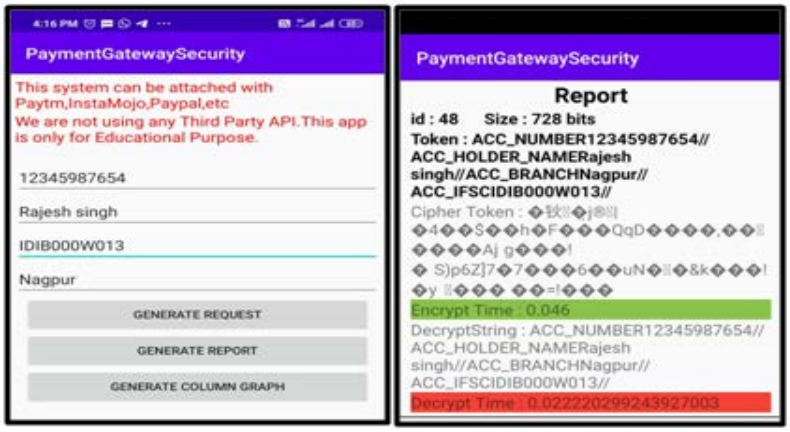

Fig. 9: Report generation-2

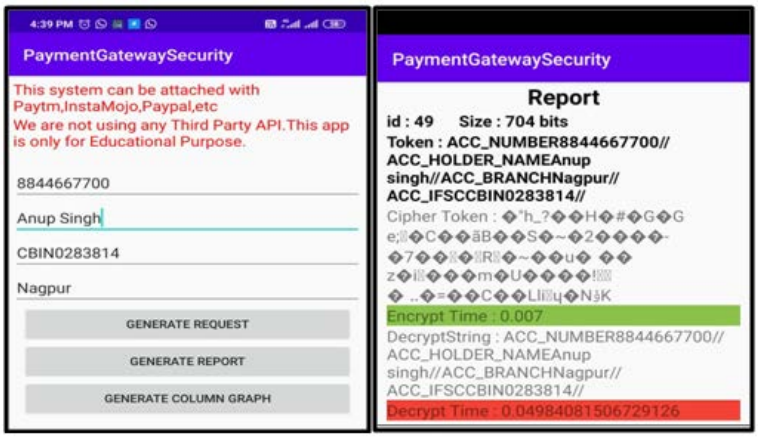

Fig. 10: Report generation-3

Table 1: Result analysis of proposed hybrid system

Proposed algorithm	Id	Message size (Bits)	Encryption time	Decryption time
Blowfish+RSA	47	760	0.009	0.05
	48	728	0.046	0.022
	49	704	0.013	0.05
	51	712	0.005	0.03

Table 2: Existing available data using hybrid system

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

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 (Fig. 11, 12, Table 1 and 2).

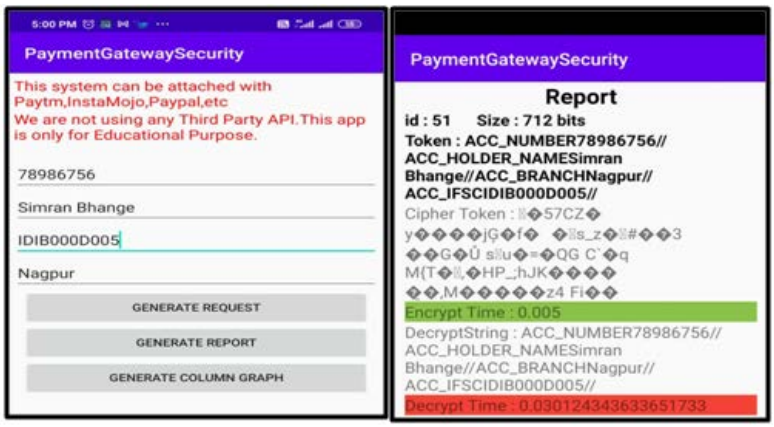

Fig. 11: Report generation-4

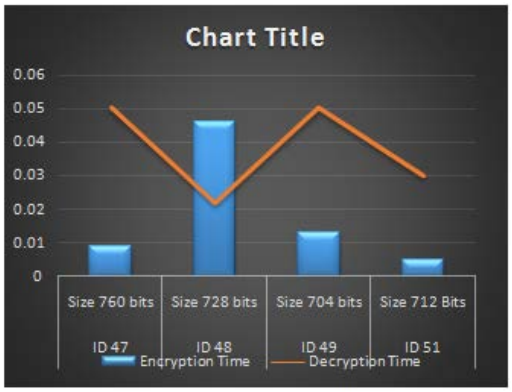

Fig. 12: Result analysis of proposed hybrid system

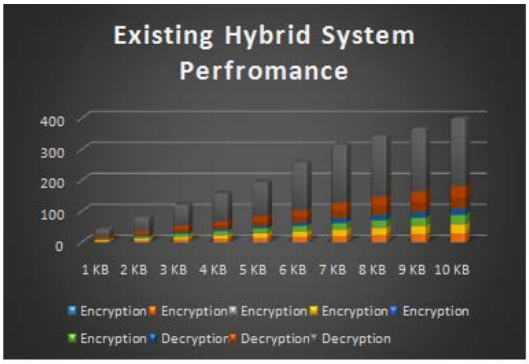

Fig. 13: Existing hybrid system performance

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.

CONCLUSION

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:

- Processor
- Key size
- Encryption time
- Decryption time
- Response from server

REFERENCES

01. Nadeem, A. and M.Y. Javed, 2005. A performance comparison of data encryption algorithms. Proceedings of the 2005 International Conference on Information and Communication Technologies, August 27-28, 2005, IEEE, Karachi, Pakistan, pp: 84-89.

02. Ramesh, A. and A. Suruliandi, 2013. Performance analysis of encryption algorithms for information security. Proceedings of the 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), March 20-21, 2013, IEEE, Nagercoil, India, pp: 840-844.
03. Prasetyo, K.N., Y. Purwanto and D. Darlis, 2014. An implementation of data encryption for internet of things using blowfish algorithm on FPGA. Proceedings of the 2014 2nd International Conference on Information and Communication Technology (ICoICT), May 28-30, 2014, IEEE, Bandung, Indonesia, pp: 75-79.
04. Minni, R., K. Sultania, S. Mishra and D.R. Vincent, 2013. An algorithm to enhance security in RSA. Proceedings of the 2013 4th International Conference on Computing, Communications and Networking Technologies (ICCCNT), July 4-6, 2013, IEEE, Tiruchengode, India, pp: 1-4.
05. Yellamma, P., C. Narasimham and V. Sreenivas, 2013. Data security in cloud using RSA. Proceedings of the 2013 4th International Conference on Computing, Communications and Networking Technologies (ICCCNT), July 4-6, 2013, IEEE, Tiruchengode, India, pp: 1-6.