DEVELOPING A NOVEL APPROACH OF HYBRID ENCRYPTION BY ECDH AND OPTIMIZE BLOWFISH FOR CLOUD DATA

Raghav Mittal

ABSTRACT

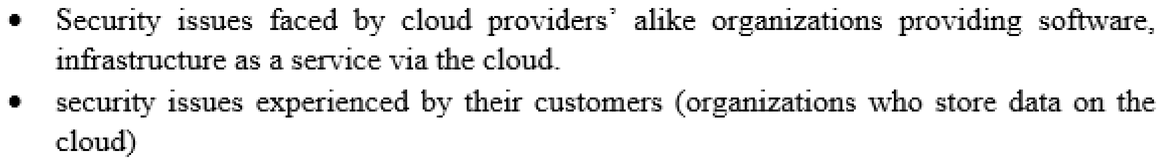
From the last few years, the scope of cloud computing is increased more. With the improvement in the field of distributed computing, there is additionally the need to verify the information by utilizing concentrated assets. The significant test in distributed computing is to give security, respectability, and dependability to the client's information. Cloud computing is an effective field for IT specialists due to its potential for transformation in the computer industry. Unfortunately, there are also some issues to be resolved and the security aspects in this field, which remain at the core of interest. The point of this exploration is to recognize and understand the security issues identified with the distributed computing. A detailed literature review is done to study the approaches and concepts used in the field of cryptography in the cloud environment. In this work, the input is given by using the Benchmark dataset, and then the key is created by using the encryption algorithm Elliptic curve and Defi Hell Men and then concatenate the keys. Optimize the AES algorithm is hybrid with Blowfish to optimize the results after this decryption process is also performed to decode the data. At last, performance evaluation of the proposed system is done by using analysis of storage and time consumed during the encryption and decryption process. The results show the attack is reduced by ECDH approach with integrity MD5.

Keywords: MD5, Optimization, AES, Blowfish

I. INTRODUCTION

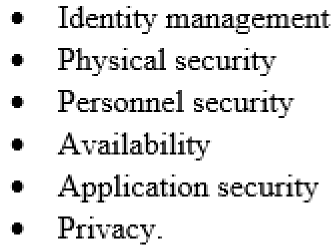
Distributed computing is seen as on-demand figuring, which is valiant of electronic enlisting that direct shared getting ready resources and data to PCs and various devices on interest. This model is enabled across the world, on-wanting access to an ordinary pool of dealing with figuring sources. Conveyed figuring and limit publications of action outfit clients and endeavors with diverse capacities to shop and technique their statistics in pariah server ranches. Conveyed figuring provides clients and adventure capability to store and method in pariah server ranches. Nowadays, appropriated figuring is seen as a completely unique locale that supplies dynamically versatile corporations and on strength over the net alongside the virtualization of equipment and programming. Conveyed registering offers security comprise into mild of the way that the pro affiliation can erupt the statistics; this is within the cloud at something factor. It is able to eliminate the facts deliberately. In a cloud, the company shared levels by using various customers. There may be a probability that records having a spot with precise customers lives on equivalent records server. In this way, information got away by accident whilst one consumer statistics is given to another.

There are various types of safety troubles related to cloud computing but fall into vast classes:



- Security issues faced by cloud providers' alike organizations providing software, infrastructure as a service via the cloud.
- security issues experienced by their customers (organizations who store data on the cloud)

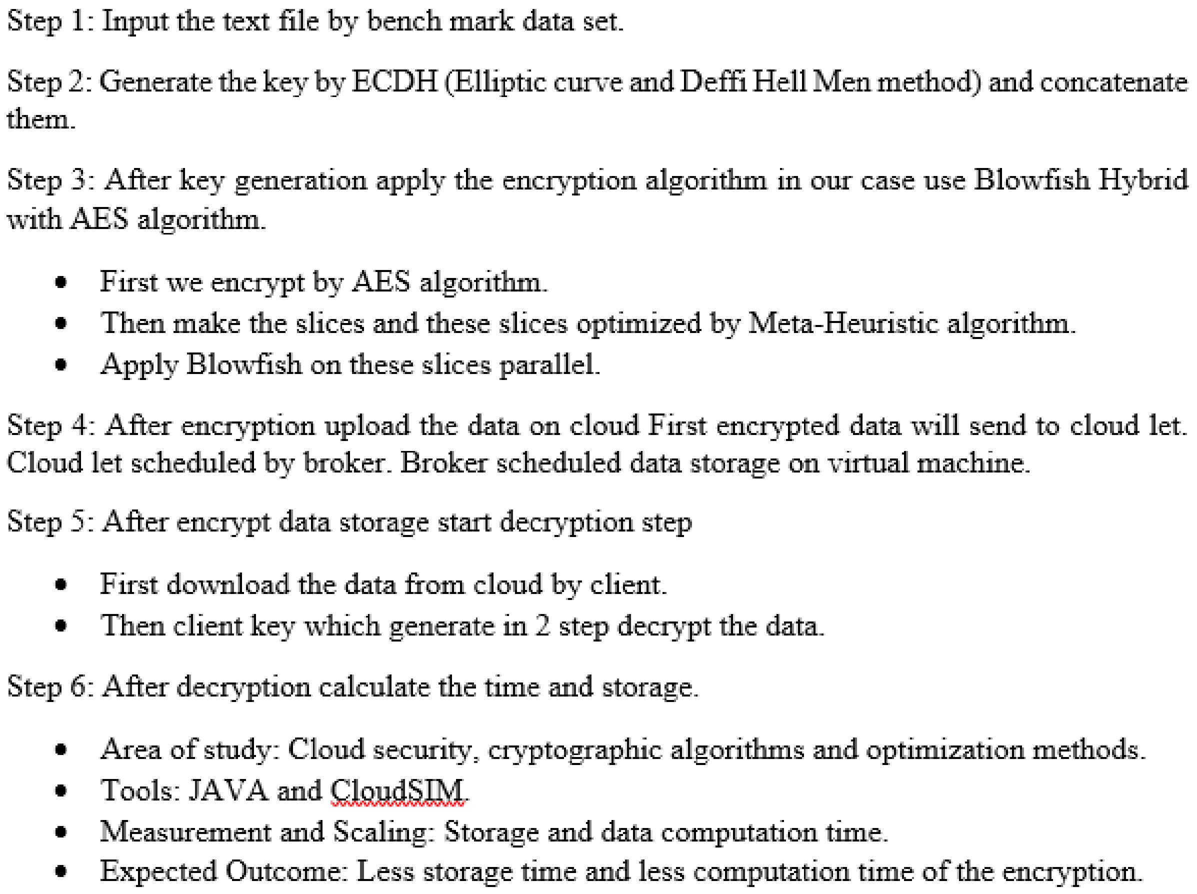
The provider issuer must make sure the secured infrastructure and programs are blanketed even though the person should take dimensions to reinforce their software and use strong passwords and authentication measures. A number of the main functions in providing facts security and integrity:



- Identity management
- Physical security
- Personnel security
- Availability
- Application security
- Privacy.

Cryptography in the cloud takes into consideration verifying basic information past your corporate IT condition, where that information is never again heavily influenced by you. Cryptography master Ralph Spencer Poore clarifies that "information in motion and information at rest are best protected by cryptographic security measures. In the cloud, we don't have the luxury of having actual physical control over the storage of information, so the only way we can ensure that the information is protected is for it to be stored cryptographically, with us maintaining control of the cryptographic key."

III. PROPOSED METHODOLOGY



Step 1: Input the text file by bench mark data set.

Step 2: Generate the key by ECDH (Elliptic curve and Deffi Hell Men method) and concatenate them.

Step 3: After key generation apply the encryption algorithm in our case use Blowfish Hybrid with AES algorithm.

- First we encrypt by AES algorithm.
- Then make the slices and these slices optimized by Meta-Heuristic algorithm.
- Apply Blowfish on these slices parallel.

Step 4: After encryption upload the data on cloud First encrypted data will send to cloud let. Cloud let scheduled by broker. Broker scheduled data storage on virtual machine.

Step 5: After encrypt data storage start decryption step

- First download the data from cloud by client.
- Then client key which generate in 2 step decrypt the data.

Step 6: After decryption calculate the time and storage.

- Area of study: Cloud security, cryptographic algorithms and optimization methods.
- Tools: JAVA and CloudSIM
- Measurement and Scaling: Storage and data computation time.
- Expected Outcome: Less storage time and less computation time of the encryption.

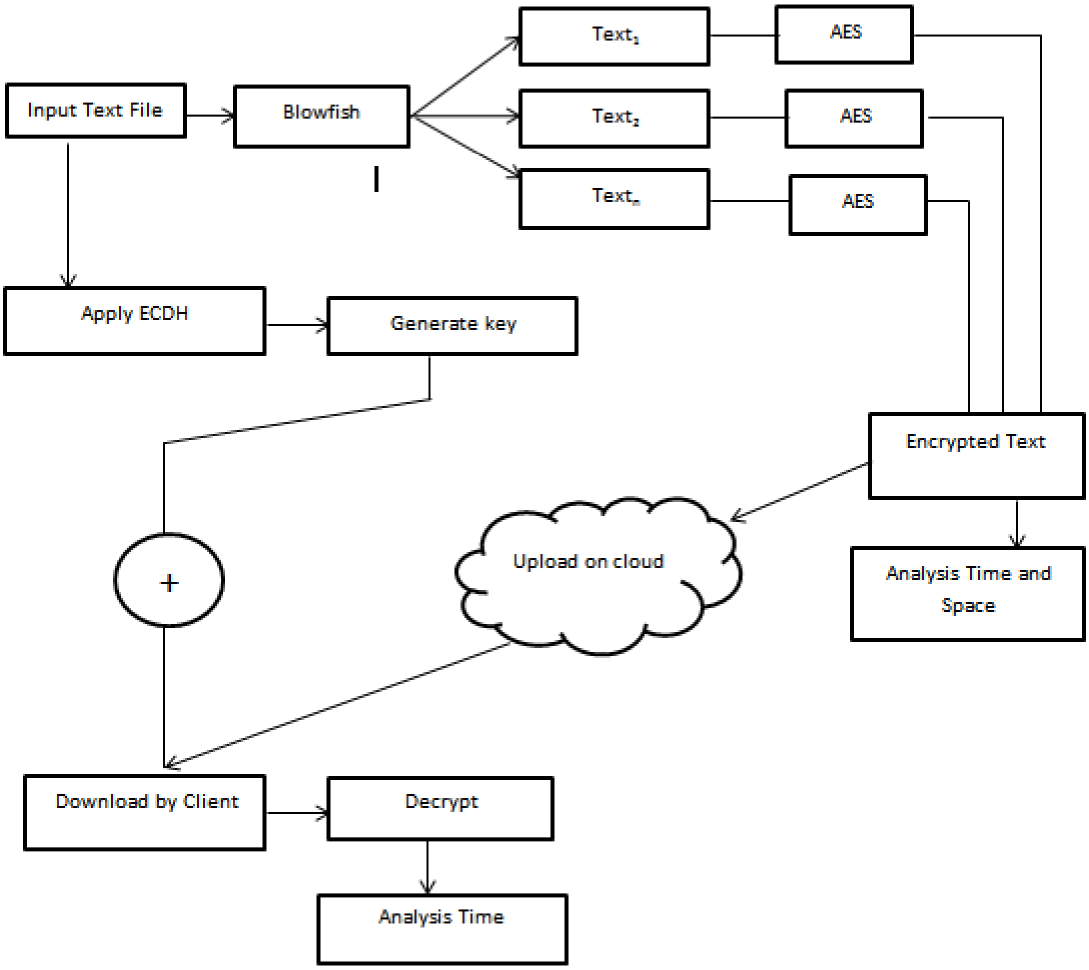
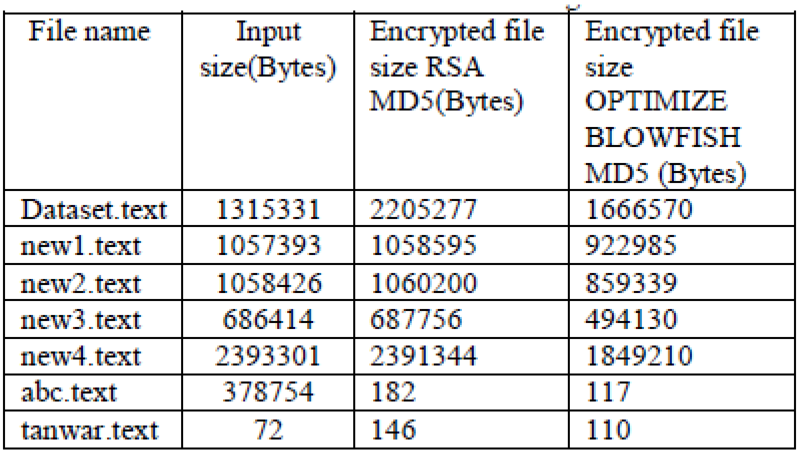


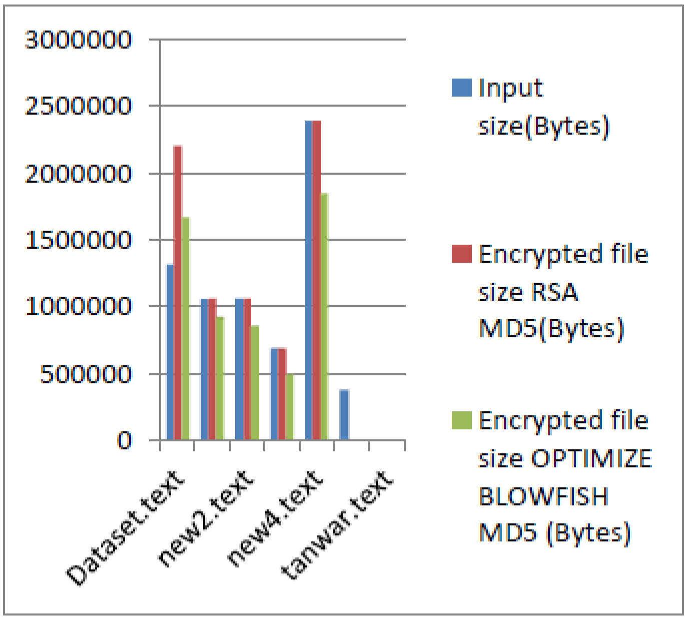
Figure 1.1 Proposed Methodology

IV. RESULTS

Beneath given tables are a relative examination of half of and half of the encryption calculation. Inside the desk, the check result encryption record length examination among Blowfish-MD5 and ECDH-AES (Elliptical Curve Diffie Hellman-advanced Encryption preferred) encryption calculation appears. With these 1/2 breed calculation correlations, the product presentation is dissected for cloud circumstances. As seemed within the above-given diagrams that the encryption and interpreting time of the half of and half of Blowfish-MD5 is lesser in comparison with the ECDH-AES calculation. desk 1.1: comparison desk of encryption document size among Blowfish-MD5 andECDH-AES set of rules



File name	Input size(Bytes)	Encrypted file size RSA MD5(Bytes)	Encrypted file size OPTIMIZE BLOWFISH MD5 (Bytes)
Dataset.text	1315331	2205277	1666570
new1.text	1057393	1058595	922985
new2.text	1058426	1060200	859339
new3.text	686414	687756	494130
new4.text	2393301	2391344	1849210
abc.text	378754	182	117
tanwar.text	72	146	110

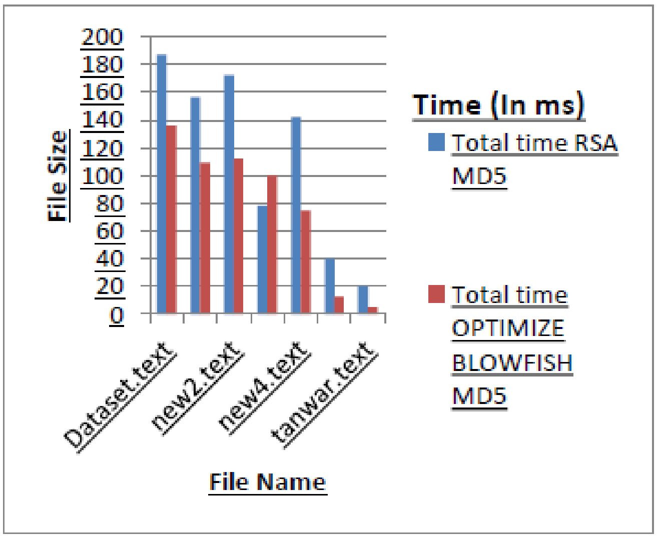


Graph 1.2: Comparison table of encryption file size between Blowfish-MD5 and ECDH-AES algorithm

The graph 4.3 shows the comparison of RSA_MD5 and Blow Fish_MD5 with file size. It shows the after encryption effect on size.

Table 1.2: evaluation table of total time among Blowfish-MD5 and ECDH-AES algorithm

File name	Input size	Total time RSA MD5	Total time OPTIMIZE BLOWFISH MD5
Dataset.text	1315331	187 ms	136 ms
new1.text	1057393	156 ms	109 ms
new2.text	1058426	172 ms	112 ms
new3.text	686414	78 ms	100 ms
new4.text	2393301	142 ms	75 ms
abc.text	378754	40 ms	13 ms
tanwar.text	72	20 ms	5ms



Graph 1.3: Comparison table of total time between Blowfish-MD5 and ECDH-AES algorithm

V. CONCLUSION AND FUTURE SCOPE

Computing on cloud is taken into consideration as a concept of cloud computing in which processing of resources and facts are shared by way of the cloud service provider. Cloud computing gives the garage area, a software program for development in statistics centers of 1/3 celebration. In this thesis, the paintings are based on the security on the cloud by way of using a hybrid set of rules. The contrast is proven among hybrid Optimize Blowfish-MD5 set of rules (proposed hybrid cryptographic algorithm) and ECDH-AES algorithm. The experimental outcomes attain shows that the proposed set of rules has lesser encryption and decryption time and needs much less garage capacity in comparison to ECDH-AES set of rules. Future prominence is given to the proposed architecture implementation evaluating with an exceptional algorithm to show their effectiveness.