Novel approach of hybrid encryption by ECDH and optimize blow fish for cloud data

Yamini Gupta[1], Sanjay[2]
Himachal Pradesh Technical University, Hamirpur, Himachal Pradesh

Abstract: From the last few years the scope of cloud computing is increased more. With the enhancement in the field of cloud computing there is also the need to secure the data by using centralized resources. The major challenge in cloud computing is to provide the security, integrity and reliability to the user's data. Cloud computing is the effective field for the IT specialists due to its potential of transformation in computer industry. Unfortunately there is also some issues to be resolved and the security aspects in this field which are remain at the core of interest. The aim of this research is to identify and solve the security issues related to the cloud computing. A detailed literature review is done to study the approaches and concepts used in the field of cryptography on cloud environment. In this work input is given by using Bench mark dataset and then key is created by using encryption algorithm Elliptic curve and Deffi Hell Men and then concatenate the keys. Optimize AES algorithm is hybrid with Blow fish to optimize the results. After this decryption process is also performed for decode the data. At last performance evaluation of the proposed system is done by using analysis of storage and time consumed during encryption and decryption process. The results show the attack is reduced by ECDH approach with integrity MD5.

Keywords: *MD5, Optimization, AES, Blow fish*

I. INTRODUCTION

Cloud computing, is recognized as on-demand computing, which is considerate of internet-based computing that administer shared processing resources and data to computers and other devices on interest. This model is enabled worldwide, on-appetite access to a shared pool of organizing computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third party data centers. Cloud computing provide users and enterprises with ability to store and process in third party data centers. Today, cloud computing is considered to be a progressive area that supply dynamically flexible services and on interest over the internet along virtualization of hardware and software. Cloud computing presents privacy involve because the service provider can outbreak the data that is in the cloud at any time. It could purposely delete the information. In a cloud, provider shared platform by various users there may be a probability that information belonging to distinct clients resides on similar data server. Therefore information escaped by mistake when one customer information is given to another.

There are various kinds of security issues associated with cloud computing but fall into two broad categories:

- 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 service provider must ensure the secured infrastructure and applications are protected although the user must take dimensions to reinforce their application and use strong passwords and authentication measures. Some of the leading features in providing data security and integrity:

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

Cryptography in the cloud employs encryption techniques to secure data that will be used or stored in the cloud. It allows users too conveniently and securely access shared cloud services, as any data that is hosted by cloud providers is protected with encryption. Cryptography in the cloud protects sensitive data without delaying information exchange.

Cryptography in the cloud allows for securing critical data beyond your corporate IT environment, where that data is no longer under your control. Cryptography expert Ralph Spencer Poore explains 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."

II. RELATED STUDY

NesrineKaaniche et al proposed an approach in which data is firstly encrypted and then stored on the public cloud server. This perception also attempt to access manage so that only recognized users can access the data. With this approach unrecognized user even not access data without client permission [1]. NehaTirthani et al interpreted about cloud security problem and then proposed a security model for cloud in which Diffie Hellman Key Exchange and Elliptical Curve Cryptography algorithms are used. The whole model is explained in four steps in which first step develops connection, the second is account formation, third is verification and last step composed of data exchange [2]. FarzadSabahi represent about the scope of migrating to the cloud. The author also explains how the migration to the cloud will benefit to organizations [3]. Deyan Chen et al explained some serious security problems with cloud computing and then supplies particulars of current security clarification for data security and privacy safeguard of cloud .[4].

Priyanka Ora suggest a solution to preserve data security and data integrity. This strategy composed of a combination of RSA Partial homomorphic and MD5 hashing algorithm .In this explanation, data is encrypted by RSA Partial before uploading it on cloud server. After it's been uploading its hash value is calculated by MD5 hashing strategy. All these perspective go through the following step Encryption/Decryption, Data uploading on a cloud, Hashing and authentication [5]. Shakeeba et al. proposed an approach, a work plan to eradictae that involve with regards to data privacy using cryptographic algorithms to advance the security in cloud as per distinct approach of cloud customers. Advantages of cloud storage are easy approach to your knowledge anyplace, anyhow, anytime, scalability, cost efficiency, and high reliability of the data. Because of these advantages each and every organization is adopting cloud, means it uses the storage service provided by the cloud provider. So there is a requirement to safeguard that data against unrecognized access, changes or denial of services etc. To protect the Cloud means to secure the calculations and storage [6]. Seny et al. describe the survey of the interests such as architecture deliver to both customers and service providers and give a summary of recent progress in cryptography inspired particularly by cloud storage. They also depict at a high level, various kinds of architectures that adjoin recent and non-standard cryptographic essential in order to achieve our goal [7].

Prof SwarnalataBollavarapu et al This paper suggest the algorithms used to store data security in the cloud and desktops and to conquered these issues encryption and decryption techniques like RSA and RC4 has been considered here in more details. The server and the email management software is installed on the cloud and managed by service providers. Delivering easy access to work and business still it has a major issue and threat i.e. "DATA SECURITY". Cloud has single layer security architecture and demand is high for customers. They can have well organized computing by centralized data storage, processing and bandwidth [8]. Akash Kanthale et al. With the fantastic growth of sensitive information on cloud, cloud storage security is becoming more important than even before. The cloud data and its services reside in relatively scalable data centres and can be accessed from everywhere. The growth of the cloud users has been accompanied with a growth in malicious activities in the cloud. More and more vulnerabilities are getting discovered, and nearly every day, new upcoming security advisories are published. Millions of users are surfing the Cloud system for various purposes, therefore they need purely safe and persistent services. The future of cloud, especially in extending the range of applications, involves a much higher degree of privacy, and authentication. Any technology can't be said perfect until it is 100% free from any vulnerability. So whenever a new technology is introduced the security is the first feature that is countable. There are many technologies that are used for online data storage, accessing the data at any location and provide the online usage of any software. Cloud computing is the technology that provides the online data storage and the most important services that it provides software on hiring facility [9].

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 parallely.

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.

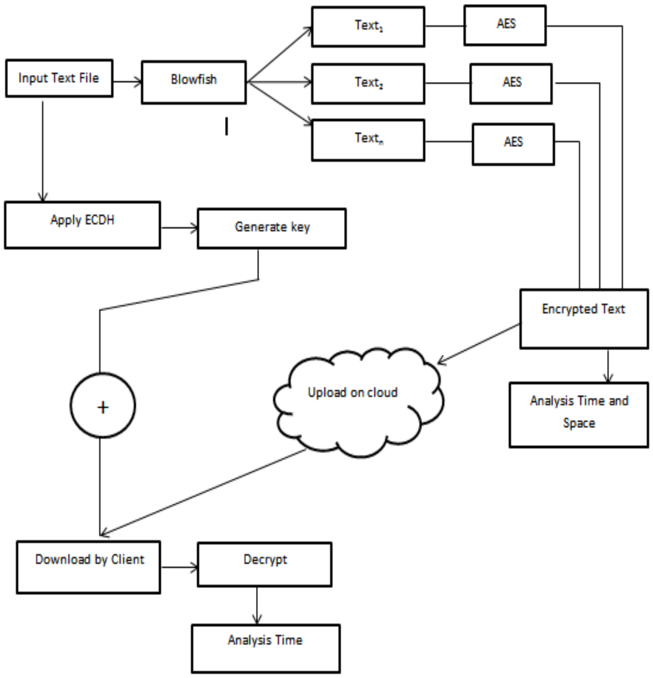


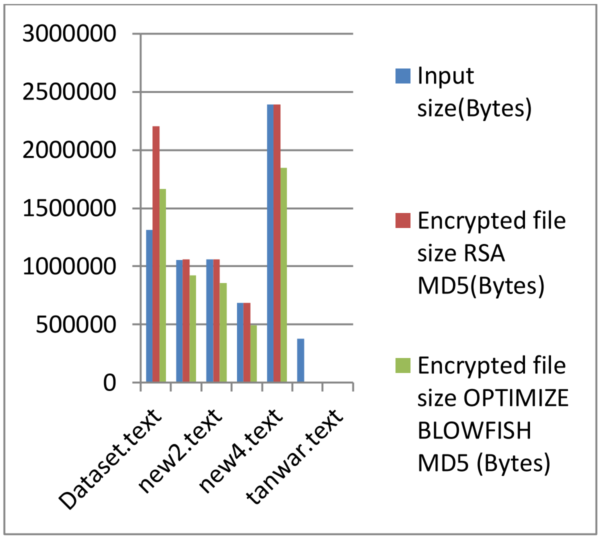
Figure 1.1 Proposed Methodology

IV. RESULTS

In below given tables is comparative analysis of hybrid encryption algorithm. In table, the experiment result encryption file size comparison between Blowfish-MD5 and ECDH-AES (Elliptical Curve Diffie Hellman-Advanced Encryption Standard) encryption algorithm is shown. With these two hybrid algorithm comparison, the efficient performance is analyzed for cloud environment.

Table 1.1: Comparison table of encryption file size between Blowfish-MD5 and ECDH-AES algorithm

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

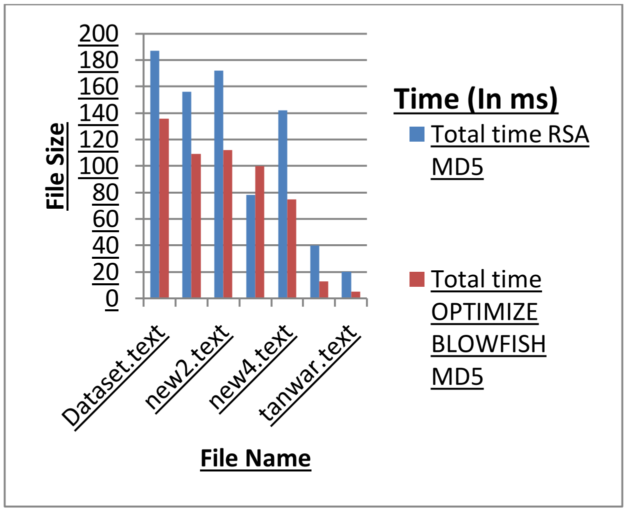


Graph 1.2: Comparison table of encryption file size between Blowfish-MD5 and ECDH-AES algorithm

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: Comparison table of total time between 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

As shown in the above given graphs that the encryption and decryption time of the hybrid Blowfish-MD5 is lesser in comparison to the ECDH-AES algorithm.

V. CONCLUSION AND FUTURE SCOPE

Computing on cloud is considered as a concept of cloud computing in which processing of resources and data are shared by the cloud service provider. Cloud computing provides the storage space, software for development in data centers of third party. In this thesis, the work is based on the security on cloud by using hybrid algorithm. The comparison is shown between hybrid Optimize Blowfish-MD5 algorithm (proposed hybrid cryptographic algorithm) and ECDH-AES algorithm. The experimental results obtain shows that the proposed algorithm have lesser encryption and decryption time and needs less storage capacity in comparison to ECDH-AES algorithm. With future prominence is given to the proposed architecture implementation comparing with different algorithm to show their effectiveness.

VI. REFERENCES

[1]. NesrineKaaniche,AymenBoudguiga, Maryline Laurent, "ID Based Cryptography for Secure Cloud Data Storage,"Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference

[2]. NehaTirthani, GanesanR,"Data Security in Cloud Architecture Based on diffie Hellman and Elliptical Curve Cryptography," International Association for Cryptologic Research, Nov 2013.

[3]. FarzadSabahi,"Cloud computing Security threats and responses "Communication Software and Networks(ICCSN).2011 IEEE 3rd International Conference.

[4]. DeyanChen,Hong Zhao," Data Security and Privacy Protection Issues in Cloud Computing, " 2012 IEEE International Conference on Computer and Electronics engineering.

[5]. Priyanka Ora and Dr.P.R.Pal, "Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography" IEEE International Conference on Computer 2015.

[6]. Shakeeba S. Khan ,Prof.R.R. Tuteja, Security in Cloud Computing using Cryptographic Algorithms, Vol. 3, Issue 1, January 2015

[7]. Seny Kamara and Kristin Lauter," Cryptographic Cloud Storage," June 2010.

[8]. Prof SwarnalataBollavarapu, Bharat Gupta, 'Data Security in Cloud Computing', Volume 4, Issue 3, March 2014

[9]. ZhaoYong-Xia and Zhen Ge ,"MD5 Research," Second International Conference on Multimedia and Information Technology, 2010

[10]. [10] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan and Tang Chaojing, "Data Security Model for Cloud Computing," Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) Qingdao, China, November 21-22, 2009.