IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue4)
Available online at www.ijariit.com

Data Security in Cloud Computing Based On Blowfish with Md5 Method

Pooja Devi
Computer Science &Engineering.
Maharaja Agrasen University
tanwarpoojacse4@gmail.com

Amit Verma
Computer Science &Engineering.
Maharaja Agrasen University
verma0152@gmail.com

Abstract— In this paper work on cloud base security, which is essential now days. Today scenario high computation speed and storage is industry or organization requirement for that they use cloud for storage but cloud will access by any number of user. SO data should be secure with minimum cost. Here cost means storage and time. Propose work reduce the storage and time in significant manner.

Keywords— Security, Blow Fish, Md5, Encryption.

I. Introduction

Cloud computing, is perceived as on-demand computing, which is considerate of web based computing that manage shared handling assets and information to PCs and different gadgets on interest. This model is empowered worldwide, on-craving access to a common pool of sorting out computing resources. Cloud computing and capacity solutions give clients and undertakings different abilities to store and process their information in outsider server farms. Cloud computing furnish clients and undertakings with capacity to store and process in outsider server farms. Today, cloud computing is considered to be a dynamic region that supply progressively adaptable administrations and on enthusiasm over the web along virtualization of equipment and programming. These days, Cloud computing is a developing region in distributed computing that convey powerfully versatile administrations on demand over the web through virtualization of equipment and programming. The greatest favourable position of the cloud is its adaptability to rent and discharge assets according to the client prerequisite. Moreover, the cloud supplier offer two sort of arrangements to be specific here and now anticipate demand and long term reservation arrange. It has astute framework i.e. Transparency, Scalability, Monitoring and Security [1].

Types of cloud computing

IT individuals talk about three various types of cloud computing, where distinctive services are being accommodated you. Take note of that there's a certain amount of vagueness about how these things are characterized and some overlap between them.

- **infrastructure as a Service (IaaS)** means you're purchasing access to raw computing hardware over the Net, for example, servers or storage. Since you purchase what you need and pay-as-you-go, this is frequently alluded to as utility computing. Ordinary web facilitating is a basic example of IaaS: you pay a month to month membership or a for each megabyte/gigabyte charge to have a facilitating company serve up documents for your site from their servers.

- **Software as a Service (SaaS)** means you utilize a total application running on another person's framework. Electronic email and Google Documents are perhaps the best-known examples. Zoho is another notable SaaS supplier offering a variety of office applications on the web.

- **Platform as a Service (PaaS)** means you create applications utilizing Web-based apparatuses so they keep running on frameworks software and hardware given by another company. In this way, for example, you may build up your own particular web based business site yet have the entire thing, including the shopping basket, checkout, and payment mechanism running on a merchant's server. App Cloud (from salesforce.com) and the Google App Engine are examples of Pa.

Cloud computing is a developing example, exchanging the capacity abilities to autonomous specialist co-ops. As a result of the loss of direct control on outer information, clients are disinclined for tolerating cloud administrations. To construct a sheltered cloud computing system, service stages and application programming levels must be considered for ensured cloud computing framework. Data encryption is one of the sufficient intends to accomplish cloud computing data security. Users can encode information that is put away or handled inside the cloud to anticipate unapproved access. Traditionally, the primary point of convergence is scrambled data on determined stage, for example, information encryption. For cloud computing, a framework level plan must be executed.

Cryptography was the uncommon area of military and administrative mystery benefits, and has been given security properties, for example, information secrecy and information root authentication. A essential contrast between cryptographic plans determines the connection between the match of keys, incorporated into message encryption and unscrambling calculations. Symmetric or ordinary cryptography rely on upon the key between two imparting elements Alice and Bob. The premise of symmetric cryptography, and additionally lopsided cryptography, is on utilizing two comparative calculations for message encryption and unscrambling Inspite of, basic operations of encryption and decryption, cryptography in cloud computing likewise supplies numerous security related capacities.

II. LITERATURE REVIEW

NesrineKaaniche et al[1]Author proposed an approach in which data is initially encoded and then put away on the general population cloud server. This discernment likewise endeavor to get to oversee so that lone perceived clients can get to the data. With this approach unrecognized client even not get to data without customer consent.

NehaTirthani et al[2]This paper translated about cloud security issue and then proposed a security demonstrate for cloud in which Diffie Hellman Key Exchange and Elliptical Curve Cryptography calculations are utilized. The entire model is clarified in four stages in which initial step creates association, the second is record arrangement, third is confirmation and last stride made out of data exchange.

FarzadSabahi[3] Author speak to about the extent of relocating to the cloud. The creator additionally discloses how the movement to the cloud will event to associations.

Deyan Chen et al.[4] clarified some genuine security issues with cloud computing and then supplies particulars of current security illumination for data security and protection shield of cloud.

Priyanka Ora and Dr.P.R.Pal [5]In this paper the creator propose an answer for preservedata security and data trustworthiness. This strategy made out of a mix of RSA Partial homomorphic and MD5 hashing calculation .In this clarification, data is scrambled by RSA Partial before transferring it on cloud server. After its beenuploading its hash esteem is ascertained by MD5 hashing strategy. All these point of view experience the accompanying stride Encryption/Decryption, Data transferring on a cloud, Hashing and confirmation.

Shakeeba S. Khan andProf.R.R.Tuteja [6]Authorproposed an approach,a work plan to eradictae that include with respect to data protection utilizing cryptographic calculations to propel the security in cloud according to particular approach of cloud clients. Advantagesof cloud stockpiling are simple way to deal with your insight wherever, in any case, whenever, scalability, cost efficiency, and high reliability of the data. As a result of these preferences every single association is embracing cloud, implies it utilizes the capacity benefit given by the cloud supplier. So there is a necessity to protect that data against unrecognized get to, changes or disavowal of administrations and so on. To ensure the Cloud intends to secure the estimations and capacity.

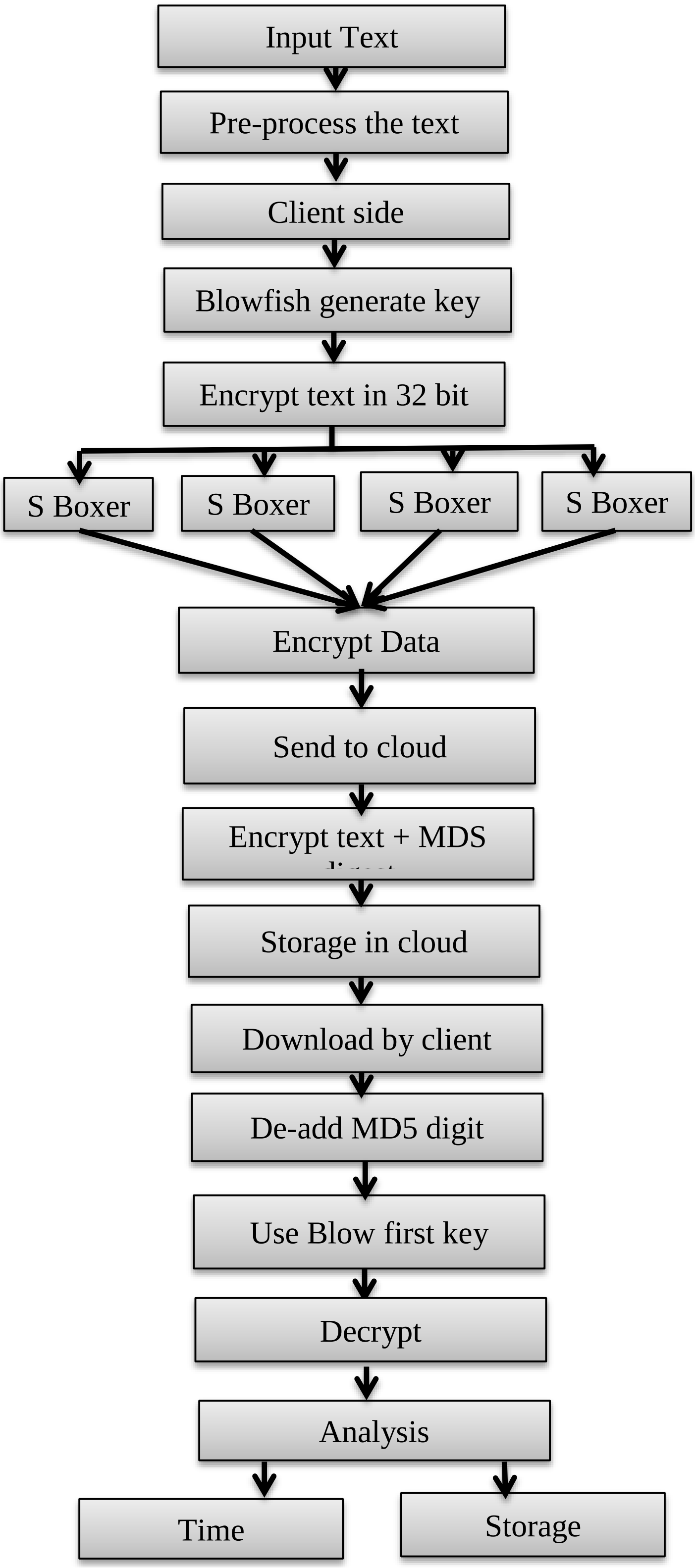
Seny Kamara and Kristin Lauter [7] depict the overview of the interests, for example, engineering convey to both clients and specialist organizations and give an outline of late advance in cryptography inspiredparticularly by cloud stockpiling. They likewise delineate at a high level, different sorts of designs that border later and non-standard cryptographic basic with a specific end goal to accomplish our objective.

Prof SwarnalataBollavarapu, Bharat Gupta[8] This paper propose the calculations used to store data security in the cloud and desktops and to vanquished these issues encryption and unscrambling strategies like RSA and RC4 has been considered here in more points of interest. The server and the email administration programming is introduced on the cloud and overseen by specialist co-ops. Conveying simple access to work and business still it have a noteworthy issue and risk i.e. "DATA SECURITY". Cloud has single layer security design and demand is high for clients. They can have efficient computing by brought together data stockpiling, handling and bandwidth.

III. METHDOLOGY

Step 1: Input the content and the info content is prepared by utilizing Blowfish calculation.
Step 2: On the customer side, encryption key is created utilizing calculation.
Step 3: Block symmetric calculation is utilized for information encryption (32 bit piece).
Step 4: The scrambled information is being transferred on to the cloud.
Step 5: Message process of the scrambled content is made by utilizing MD5 calculation and put away in the cloud.
Step 6: The customer downloads the content from the cloud and unscramble by utilizing Blowfish and MD5 calculation.

Step 7: Finally, the execution time and capacity size is being broke down and contrasted and ECDH-AES calculation.



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.

© 2017, www.IJARIIT.com All Rights Reserved

Table 1: Encryption file size of Blowfish-MD5 algorithm

File name	Input size	Encrypted file size BLOWFISH MD5
Dataset.text	1216841 Bytes	1666570 Bytes
new1.text	581469 Bytes	922985 Bytes
new2.text	581632 Bytes	859339 Bytes
new3.text	378754 Bytes	494130 Bytes
new4.text	1315331Bytes	1849210 Bytes
abc.text	89 Bytes	117 Bytes
tanwar.text	72 Bytes	110 Bytes

Graph 1: Encryption file size of Blowfish-MD5 algorithm

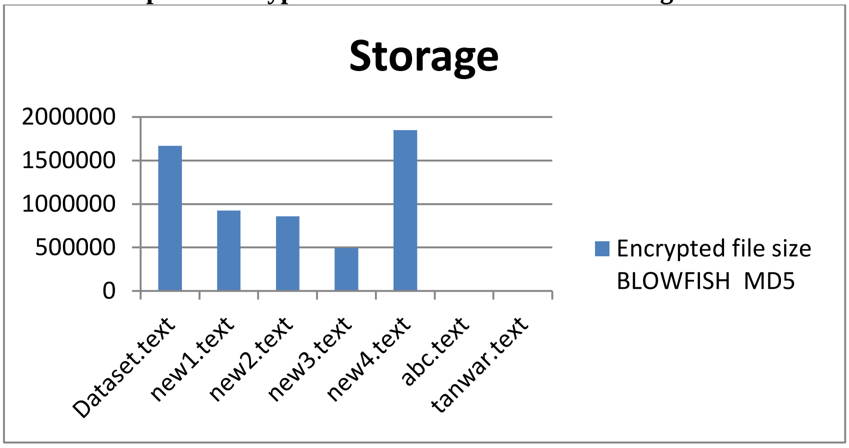
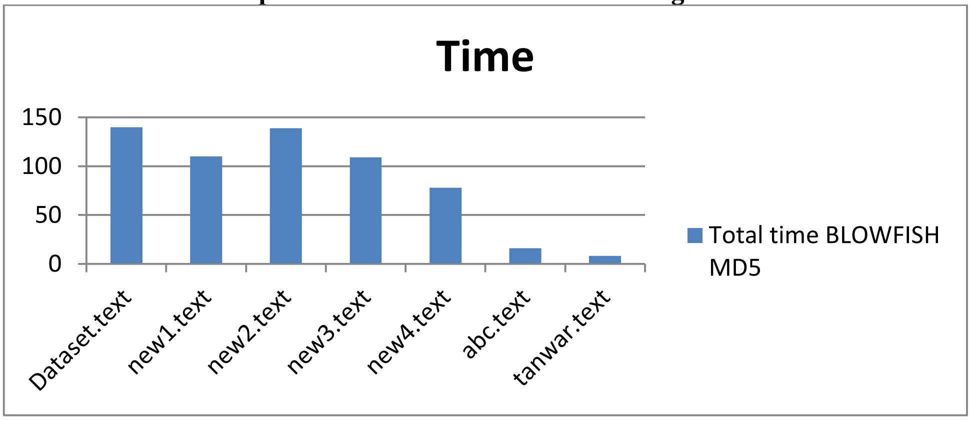


Table 2: Total time of Blowfish-MD5 algorithm

File name	Input size	Total time BLOWFISH MD5
Dataset.text	1216841 Bytes	140 ms
new1.text	581469 Bytes	110 ms
new2.text	581632 Bytes	1139 ms
new3.text	378754 Bytes	109 ms
new4.text	1315331Bytes	78 ms
abc.text	89 Bytes	16 ms
tanwar.text	72 Bytes	8 ms

Graph 2: Total time of Blowfish-MD5 algorithm



© 2017, www.IJARIIT.com All Rights Reserved

Table 3: Comparison table of encryption file size between the Blowfish-MD5 and ECDH-AES algorithm.

File name	Input size	Encrypted file size ECDHAES	Encrypted file size BLOWFISH MD5
Dataset.text	1216841 Bytes	2205277 Bytes	1666570 Bytes
new1.text	581469 Bytes	1058595 Bytes	922985 Bytes
new2.text	581632 Bytes	1060200 Bytes	859339 Bytes
new3.text	378754 Bytes	687756 Bytes	494130 Bytes
new4.text	1315331Bytes	2391344Bytes	1849210 Bytes
abc.text	89 Bytes	182 Bytes	117 Bytes
tanwar.text	72 Bytes	146 Bytes	110 Bytes

Graph 3: Comparison table of encryption file size between Blowfish-MD5 and ECDH-AES algorithm

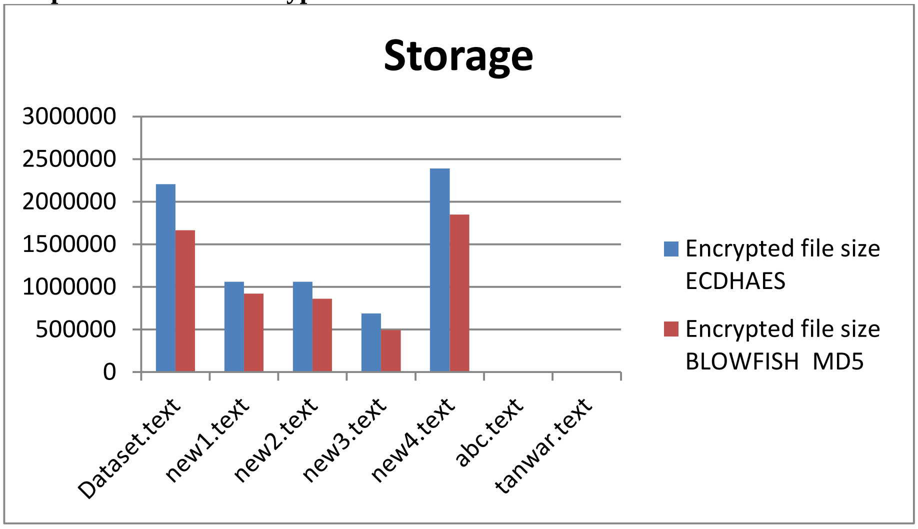
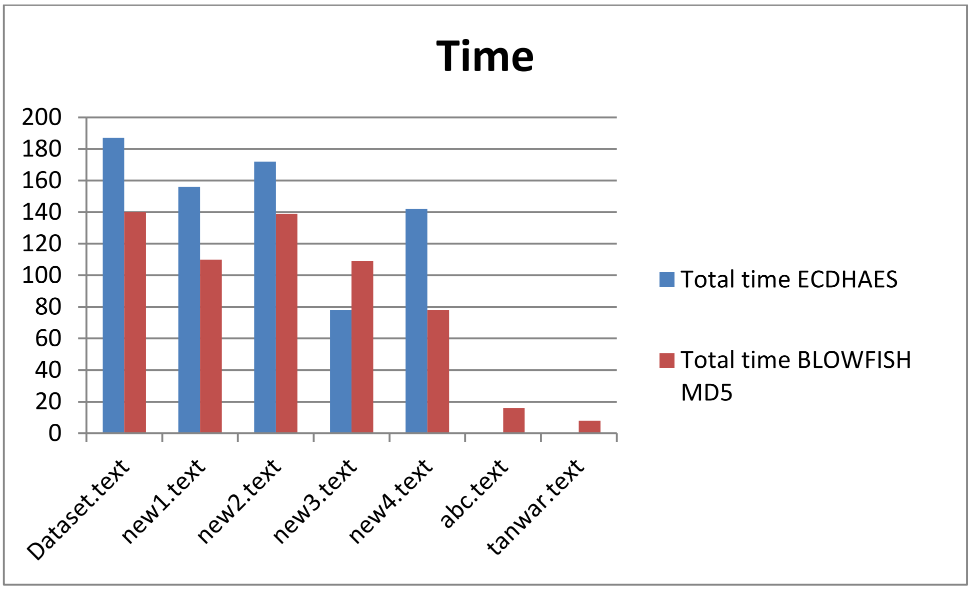


Table 4: Comparison table of total time between Blowfish-MD5 and ECDH-AES algorithm

File name	Input size	Total time ECDHAES	Total time BLOWFISH MD5
Dataset.text	1216841 Bytes	187 ms	140 ms
new1.text	581469 Bytes	156 ms	110 ms
new2.text	581632 Bytes	172 ms	1139 ms
new3.text	378754 Bytes	78 ms	109 ms
new4.text	1315331Bytes	142 ms	78 ms
abc.text	89 Bytes	0 ms	16 ms
tanwar.text	72 Bytes	0 ms	8 ms

Graph 4: 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.



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] 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.