isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 1 ,Apr,2021 ,ISSN_NO: 2321-3337

SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

Dr.M.Naveetha Krishnan Ph.D., Head of the Department, Department of computer Science.

Mr.T.Tamilarasan, Student of Computer Science department ,

St. Joseph College of Engineering, Sriperumbudur, Chennai

Abstract

As an emerging technology and business paradigm, Cloud computing platforms provide easy access to a company's high-performance, computing and storage infrastructure through web services. Mainly cloud computing technology enables users/enterprises to eliminate the requirements for setting up of expensive computing infrastructure and reduces system's operating costs. Data security and privacy are increasingly becoming the predominant issue that affects small and medium business organizations' readiness to migrate their data from on-site to cloud storage facilities. As a result, this technology is used by an increasing number of end users. On the other hand, existing security deficiencies and vulnerabilities of underlying technologies can leave an open door for intrusions. Therefore, cloud computing providers need to protect their user's sensitive data from insider or outsider attacks by installing an intrusion detection system. Form the viewpoint of security, Deduplication, various risks and issues are identified in the area of Cloud Computing. There are various risks associated with the security but one of the major issues is the security of data being stored on the provider's cloud and privacy while the data is being transmitted. This paper deals with various issues associated with security and focus mainly on the data security and methods of providing security by data encryption. Various encryption methods of block cipher algorithms such as Triple DES, Blowfish are discussed for providing solutions to cloud

1. Introduction

A. Cloud Computing Background

Data is a collection of information, is a familiarity, awareness, or understanding of someone or something such as facts, information, descriptions, or skills, which is acquired through experience or education by per ceiving, discovering or learning. Knowledge can refer to a theoretical or practical understanding of a subject. cloud computing utilizes existing internet infrastructure to facilitate communication between client nodes and services or applications that reside on a remote server

It can be implicit (as with practical skill or expertise) or explicit (as with the theoretical understanding of a subject); it can be more or less formal or systematic. Data acquisition involves complex cognitive processes: perception, communication, and reasoning; while knowledge is also said to be related to the capacity of acknowledgement in human beings. There exists the need for collecting, gathering and managing the information.

B. Aims and Objectives

- To investigate current perceptions regarding the security of cloud storage.
- To analyze the implementation of hybrid cryptography as it pertains to securing file storage on cloud infrastructure.
- Investigate the future direction of hybrid cryptographic techniques on securing data, information, and services residing on cloud infrastructure.

2. Literature Survey

Data Security Issues are main issue in the existing system. Due to openness and multi-tenant characteristics of the cloud, the traditional security mechanisms are no longer suitable for applications and data in cloud. Some of the issues are as following:

- Due to dynamic scalability, service and location transparency features of cloud computing model, all kinds of application and data of the cloud platform have no fixed infrastructure and security boundaries. In the event of security breach, it is difficult to isolate a

particular resource that has a threat or has been compromised.

- According to service delivery models of Cloud computing, resources and cloud services may

be owned by multiple providers. As there is a conflict of interest, it is difficult to deploy a unified security measure.

- Due to the openness of cloud and

sharing virtualized resources by multitenant, user data may be accessed by other unauthorized users.

Knowledge management is the systematic management of an organizations knowledge assets for the purpose of creating value and meeting tactical and strategic requirements, it consists of the initiatives, processes, strategies and systems that sustain and enhance the storage, assessment, sharing, refinement, and creation of Knowledge. The Previous chapter discuss about the process of gathering the knowledge from various sources like education sector

A. Current Perceptions Regarding the Security of Cloud Storage

There is no doubt that the emergence and increased uptake of cloud storage services by small and medium businesses (SMBs) has changed. how they conduct business. SMBs have indeed reported reaping various benefits such as cost savings, limited data redundancy and duplication, and protection against malware.

The survey reveals a wide range of prevailing negative perceptions regarding the security of cloud-based storage services. For example, the survey shows that an estimated 61% of SMBs situated across the U.K. and France still believe that their organizational data is unsafe in the Cloud despite their extensive data security investment. 50% believe in the principle that cloud storage services are less safe than on-site storage facilities, while 45% contend that migrating their data to the Cloud has compromised their security.

B. Current Implementation of Hybrid Cryptography in Securing File Storage on Cloud Infrastructure

Users are Slightly Moving away from traditional storage devices such as thumb drives, hard disks, and other physical storage devices that are gradually becoming obsolete. This modification has come due to the globalization of business that has necessitated sharing data for collaborative working and using multiple personal devices.

However, another hybridization technique involves the combination of Blowfish and ECC (Elliptic Curve Cryptography), which is an emerging alternative for traditional public-key cryptosystems, such as RSA, and which a study argues is the best substitute for asymmetric encryption. ECC is in itself founded on the "toughness of the discrete logarithm problem (DLP), whose network bandwidth is little, and the public key is short. These characteristics make it difficult to guess the keys of the encryption technique and hence render it resistant to attacks.

Overall, the implementation of hybrid cryptographic techniques is better than implementing either symmetric and asymmetric cryptography. In their analysis of cloud storage security, discovered that hybrid cryptography is better poised to ensure the attainment of security techniques for data protection that have been accepted universally in the field of information security.

These techniques are achieved through mechanisms of access control, authorization, authentication, and confidentiality. A 2016 study appreciates that cloud storage services subscribers can only trust the infrastructure's data protection capabilities when the prevailing data protection system the mechanisms above into account.

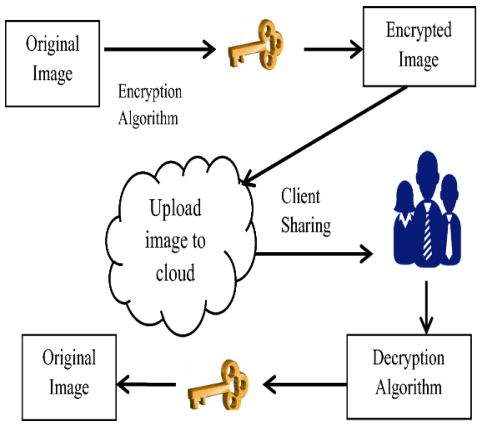
C. Future Directions for Securing File Storage on Cloud Infrastructure

Information Security experts should consider implementing high-level security by hybridizing public key cryptography. Currently, hybridization has only been applied to private key cryptography algorithms. Hence, the research recommends secrete writing to conceal the existence of secret data so that it remains invisible to the public but visible to valid receivers.

Secrete Writing may useful for text data because it enables secret data to be secured within the text's cover file. This method ensures that the text cover file resembles a normal text file and does not attract a possible attacker's interest. In the rare event that an illegitimate user finds the hidden data, they may be dispirited by the large amount of time it may take to recover it.

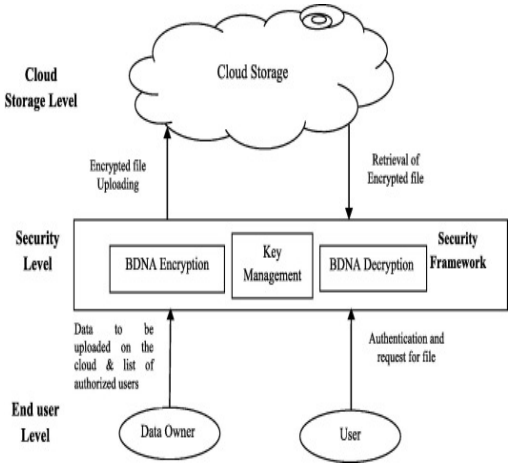
3. System Design

A conceptual framework shows the three stage of data input, process and output. Input it represents the data as input to the system that includes: student information, student transcript, and types of appeal, schedule, exam questionnaires and breakdown marks.



This data represents different dataset in the system process. it pertains to the research activities identifying needs and demands, data collection and preparation, through the use of DM model by Botha.

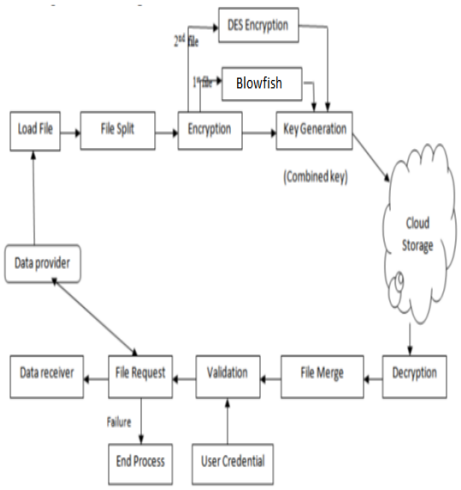
It includes also the process such as system design, development and system testing and evaluation.

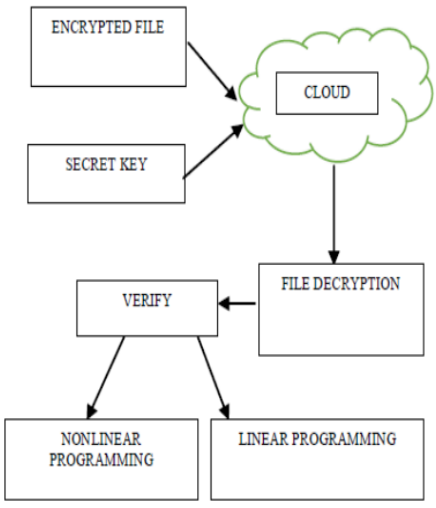


The basic role of this information sharing framework if for clients to share and use knowledge among themselves through knowledge bases. The information sharing paradigm might be

Volume: 6, Issue: 3,Special Issue: 1 ,Apr,2021 ,ISSN_NO: 2321-3337

particularly viable for application to information bases in such areas as the board handle that comprise of few sections comparing various organizations



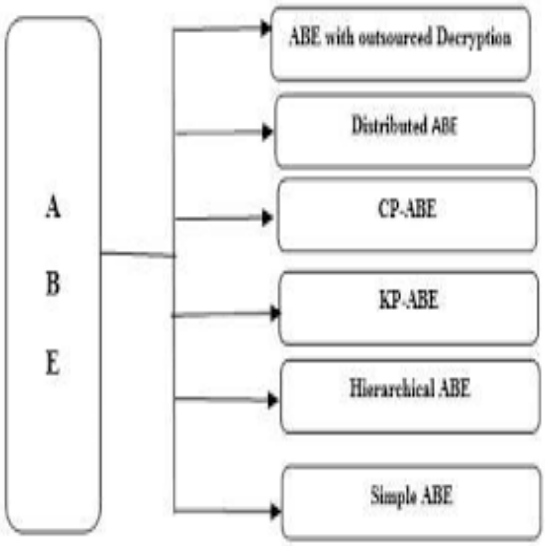


Cloud computing providing confidentiality over the insensitive data was the major issue related to security. It verifies the data owned by the server through liner computations. The proposed work enables security and efficiency using the cryptographic techniques of hybrid algorithms, securing the sensitive information that is present in the cloud. In the hybrid algorithm, it is the combination of problem encryption, key generation, result decryption and proof generation. It also validates the results which are being computed and also provides end-to-end confidentiality over the data to both the end users.

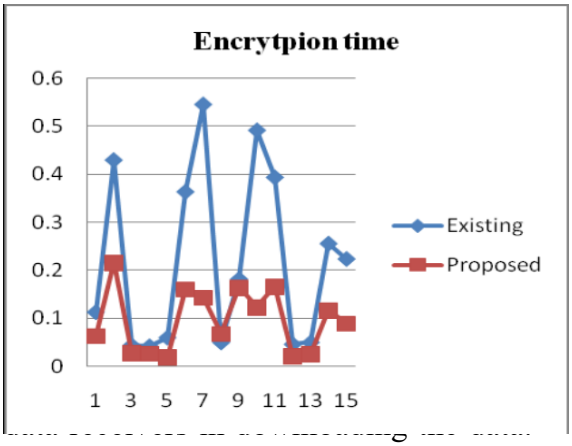
4. Implementation

The factors included in the algorithm flexibility, suitable for the algorithm process the hardware and software implementation and over all simplicity of process. The before the encryption process the method is divided into the two parts, the encryption using the data using AES for the first portion of data. The DES encrypts the second part into the finally the data stored in the cloud server.

Volume: 6, Issue: 3,Special Issue: 1 ,Apr,2021 ,ISSN_NO: 2321-3337



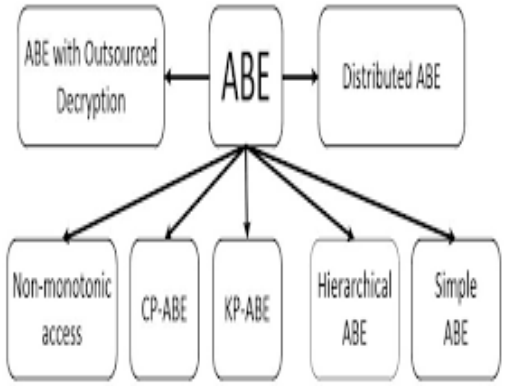
A main specification for the data receivers' needs unique file in



The downloading process uses the key and mainly valid for the downloading the data with the original format fir decryption

A comparison graph for encryption Time.

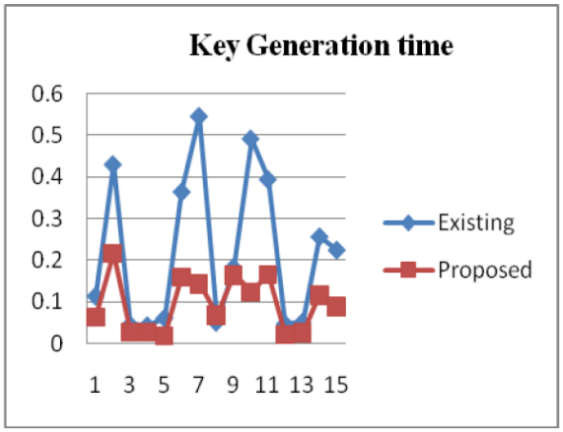
Evaluation for KP-ABE performance, time required for encryption and uploading the file on the MYSQL Database by utilizing multiple sizes of file – 1KB, 2KB, 5KB, 50KB and 100KB is considered.



Person who is still making use of antiquated DES to encrypt. Around 35 years from now, the federal government initially built DES encryption to give security of cryptographic for all kind of communications of government. Intention was to make sure that all government system should use secured and same standard in order have smooth connectivity internally.

There were some continuous sponsored

challenges conducted to understand time taken in decryption of messages. These were conducted to prove that DES was insufficient and shall not be applied in crucial system. The Electronic Frontier Foundation (EFF) and distributed.net are two firms that played vital roles to break DES.



A comparison graph for encryption Time.

Evaluation for KP-ABE performance, time required for encryption and uploading the file on the MYSQL Database by utilizing multiple sizes of file – 1KB, 2KB, 5KB, 50KB and 100KB is considered.

Time of Key generation is to generate key in file downloading process from the system. The size of file used are 1KB, 2KB, 5KB, 50KB, and 100KB. The small file not required the time for generating the secret key. The secret key uses the file downloading process

5. Conclusion and Future Enhancement

System performance is evaluated by calculating time of encryption, time of key generation and decryption time. The time consumed by KP-ABE outsourcing scheme can be measured on IDE which refers to Integrated Development Environment JAVA when the database is held in MYSQL. Performance is analyzed by calculating time of Encryption and upload, time of download and Decryption and time of key generation. With the help of multiple sizes of files, Performance analysis is performed and by taking note of encryption time of files having multiple sizes and decryption time of the files and key generation time, the results will be attained.

Hybrid cryptography systems currently use combinations of RSA and AES, AES and Blowfish, Blowfish and ECC and Triples DES among various others. Such combinations ensure that those CSPs can harness both algorithms'

advantages in a hybrid system to ensure access control, authorization, authentication, and confidentiality.

6. References

[1]. Yohannes kurniawan. The role of knowledge management system in school: perception of applications and benefits. Journal of Theoretical and Applied Information Technology, 10th March. Vol. 61 No.1(2014).

[2]. JUDITH K. LARSEN. Knowledge Utilization. Knowledge. Creation. Diffusion. Utilization, Vol I No 3, March /980421-442.

[3]. William Wagner. Issues in Knowledge Acquisition. 1990 ACM 089791-416-3.

[4]. Koech Sitienei Caroline. Knowledge Storage, Retrieval and Employee Performance: The Moderating Role of Employee Engagement. International Journal of Small Business and Entrepreneurship Research Vol.3, No.6, pp.1-13, November 2015.

[5]. Mazrekaj, A., Shabani, I. and Sejdiu, B., 2016. Pricing schemes in cloud computing: an overview. International Journal of Advanced Computer Science and Applications, 7(2), pp.80-86.

[6]. S. Carlin and K. Curran, "Cloud Computing Security", Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments, vol. 1, no. 2, pp. 12-17, 2013. Available: https://www.igi-global.com/chapter/cloud-computing-security/68920. [Accessed 8 December 2020].

[7]. Jyoti, T. and Pandi, G., 2017. Achieving Cloud Security Using Hybrid Cryptography Algorithm. International Journal of Advance Research and Innovative Ideas in Education, 3(5).

[8]. D. P. Timothy and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, 2017, pp. 1-5, doi: 10.1109/ICMDCS.2017.8211728.

[9]. Odun-Ayo, I., Ajayi, O., Akanle, B. and Ahuja, R., 2017, December. An overview of data storage in cloud computing. In 2017 International Conference on Next Generation

Computing and Information Systems (ICNGCIS) (pp. 29-34). IEEE.

[10]. "Cloud Storage Security Issues | A Research Report", IS Decisions, 2020. [Online].Available: https://www.isdecisions.com/cloud-storage-security-issues/. [Accessed: 08-Dec- 2020].

[11] Kumar, M.A. and Karthikeyan, S., 2012. Investigating the efficiency of Blowfish and Rejindael (AES) Algorithms. International Journal of Computer Network & Information Security, 4(2), p.22.

[12] Mahalle, V.S. and Shahade, A.K., 2014, October. Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. In 2014 International Conference on Power, Automation and Communication (INPAC) (pp. 146-149). IEEE.

[13] Bhandari, A., Gupta, A. and Das, D., 2016, January. Secure algorithm for cloud computing and its applications. In 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence) (pp. 188-192). IEEE.

[14] Timilsina, S. and Gautam, S., 2019. Analysis of Hybrid Cryptosystem Developed Using Blowfish & ECC with Different Key Size. Technical Journal,