iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** XII **Month of publication:** December 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Novel Approach for Cloud Data Security Enhancement through Cryptography and Biometric in the Public Cloud environment

S. Prabu[1], Prof. Gopinath Ganapathy[2]
[1]Research Scholar, [2]Professor and Head
School of Computer Science, Engineering and Applications, Bharathidasan University Tiruchirappalli - 620023, Tamil Nadu, India,

Abstract: ***Cloud computing takes the technology, services, and applications that are similar to those on the Internet and turns them into a self-service utility. It is the delivery of computing as a service rather than a product whereby shared resources, software and information is provided to computers. In these days a single server handles the multiple requests from the user. Here the server has to process the both the request from the user simultaneously, so the processing time will the high. This may leads to loss of data and packets may be delayed and corrupted and also the Data Management and the Services are not Trust Worthy. Users start worrying about losing control of their own data. Also the data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. An efficient data placement algorithm is proposed and implemented in this paper. The data placement algorithm will tell us how to place the files efficiently to the containers in object storage. Besides, the files will merge when client needs it back. So some additional algorithms are also used for partitioning and merging of files. So the objective is to achieve good security for cloud storage system, through proposed algorithm by using multiple containers of object storage in cloud. To handle these issues, the paper proposed an approach to store the data through data placement algorithm, to provide authentication and secure access control for data using Crypto-Biometric System (CBS) in cloud computing and to Protect the data from unauthorized access.***
Keywords: Cloud Computing, Crypto-Biometric System, Data Placement Algorithm.

I. INTRODUCTION

Cloud computing conveys enormously versatile registering resources as a services with Internet based advancements. Resources are shared among an incomprehensible number of customers taking into account a lower expense of IT proprietorship. At present, cloud computing is broadly examined in the technology world and industry. Virtualization, circulated registering innovation etc, cloud computing incorporates the processing, storage, organizing and other figuring resources, and afterward rents to clients. Such mode could decrease the expense of big business data development and quicken the information of big business. The Cloud storage is intended for virtualized PC environment. The cloud storage is actualized utilizing cloud computing that implies using the product and equipment resources of the cloud computing services supplier.

Cloud computing is developing at a high speed in the IT business around the globe. While there are numerous points of interest of cloud computing, the undertakings are as yet holding up to utilize cloud computing, on account of the information security issue of cloud computing is not illuminated totally. Cloud storage gives a virtual space to store mass information. Be that as it may, the information proprietors have no power over their information. The cloud supplier has full control on the client's information. This makes the client's psyche to thing about the information security in the cloud.

The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. To allay users' concerns, it is essential to provide an effective mechanism based on the notion of information accountability for users to monitor the usage of their data in the cloud.

Our contribution to addressing these problems is a Privacy Manager, which helps the user manage the privacy of their data in the cloud. As a first line of defence, the privacy manager uses a feature called obfuscation, where this is possible. The idea is that instead of being present unencrypted in the cloud, the user's private data is sent to the cloud in an encrypted form, and the processing is done on the encrypted data. The result of the processing is de-obfuscated by the privacy manager to reveal the correct result.

The obfuscation method uses a key which is chosen by the user and known by the privacy manager, but which is not communicated to the service provider. Thus the service provider is not able to de-obfuscate the user's data, and this data is not present on the service provider's machines, reducing (or even eliminating) the risks of theft of this data from the cloud and unauthorized uses of this data. Moreover, the obfuscated data is not personally identifiable information, and so the service provider is not subject to the legal restrictions that apply to the processing of the unobfuscated data.

Where obfuscation is practical, the principle of data minimization gives a legal impetus to use it. However, it is not practical for all cloud applications to work with obfuscated data. For applications for which users have to upload some private data to the cloud, the privacy manager contains two additional features, called preferences and personae, which help the users to communicate to service providers their wishes for the use of this personal data, and thus assist the service providers to respect privacy laws requiring users' consent.

The preferences feature allows users to set their preferences about the handling of personal data that is stored in an unobfuscated form in the cloud. It communicates these preferences to a corresponding policy enforcement mechanism within the cloud service. The preferences can be associated with data sent to the cloud, and preferably cryptographically bound to it (by encrypting both the policy and data under a key shared by the sender and receiver).

For stickiness of the privacy policy to the data, public key enveloping techniques can be used. Alternatively, it is possible to use policy-based encryption of credential blobs.

Part of the preference specification could involve the purpose for which the personal data might be used within the cloud, and this could be checked within the cloud before access control were granted, using mechanisms specified. The personal feature allows the user to choose between multiple personae when interacting with cloud services.

The user's choice of persona provides a simple interface to a possibly complex set of data use preferences communicated to the service provider via the preference feature, and may also determine which data items are to be obfuscated. A proposed efficient data placement algorithm is used. This will consider how to place the files efficiently to the containers in object storage. Besides, the files will merge when client needs it back. So some additional algorithms are also used for partitioning and merging of files. This paper extends the basic idea to store the data through data placement algorithm, to provide authentication and secure access control for data using Crypto-Biometric System (CBS) in cloud computing and to Protect the data from unauthorized access.

II. LITERATURE SURVEY

This paper introduced brief analysis on data security in cloud environment. It is identified and presented as challenges in data security. There are still many actual problems that need to be solved and data are migrating to public or hybrid cloud.[1].The digital signature and Diffie Hellman key exchange blended with AES encryption algorithms to protect confidentiality of data stored in cloud. It takes more time to stored or accessing data in cloud [2].The hardware consumption is minimized. For this, implementation has been made using 128-bit block size & makes open to attacks [3]. The RSA Algorithm and digital signature with encryption model is highly secured and light encryption system information has been processed [4]. Combined biometric Cryptography as crypto-biometric system was proposed to enhance the network security [5]. Enhancement of security of cloud and strong authentication has been explained in paper [6]. The key security considerations and challenges are currently faced in the cloud computing[7]. The various security algorithms, security issues and security attacks in cloud computing are discussed in paper [8]. The paper [9] deals with comparison of seven algorithms, five algorithms for symmetric algorithm and two for asymmetric algorithm for data security in cloud. Authors Compared various Security algorithms for data security in cloud computing. Based on the study of paper [10], AES was suggested as more secure and fast in speed of access wherein the AES was best but there is not practical results/examples. Implementation of AES for security over data provides benefits of less memory consumption and less computation time as compared to other algorithms which was discussed in paper[11]. The security of data is ensured by applying a method RSA algorithm.[12]. Regarding the file size reflecting only in indexing process and not affecting the data protection gives strong protection. But it is not tested with the low and medium protection technique [13].

III. METHODOLOGY

The figure 1 deals with biometric authentication that creates DB based on the features Extracted from IRIS image for the New Client. This verifies DB and Provide Authentication with the Existing Client. This results in an efficient algorithm which is the best algorithms for IRIS recognition. And AES – cryptographic random key generation which proposed with an Enhanced AES for more security and preventing attacks.

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

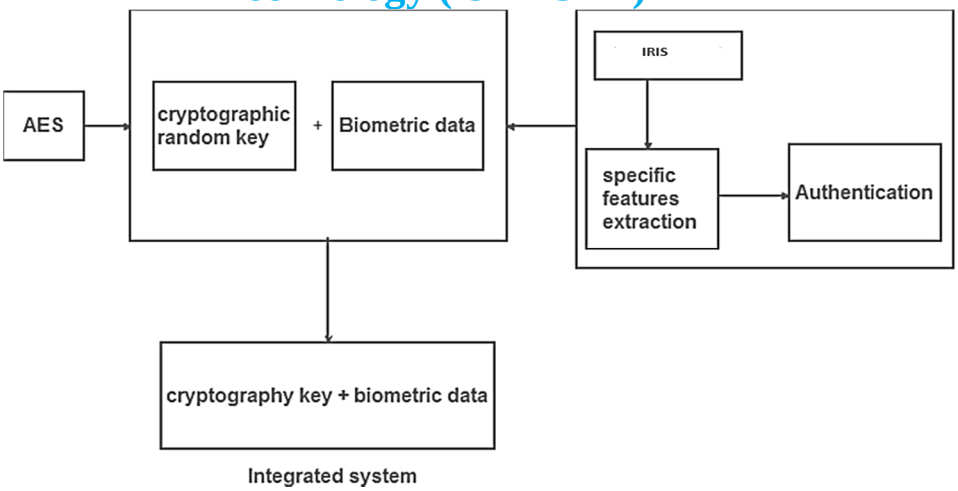


Fig.No.1. Proposed model

IV. DATA PLACEMENT ALGORITHM

In this paper, an efficient data placement algorithm is proposed. The Application is designed based on data partitioning and merging. The partitioned data can widely cloud to multiple containers of object storage in IBM Bluemix. Data placement is efficient for storage system. After determining how many files partitioned, the technique is maintain a file to move on to containers. we will consider how to place these files efficiently to containers. so the data placement algorithm is used to place files among containers in object storage. Data placement based on cloud storage has been proposed method in storage system. The proposed Idea of effective storage management scheme used in multiple containers of object storage service in IBM bluemix[14]. Many cloud storage systems applied different strategies for effective storage, but they do not consider available storage and has some other issues. In this paper, therefore an efficient data placement algorithm is proposed with some additional algorithm for data partition and merges. The cloud storage application is designed based on data partitioning[15] and widely distributed, to multiple containers of object storage in IBM bluemix cloud.

A. Algorithm

1) Data Placement Technique

CN weight = CN DiskSpace + CN Avail
CN Avail = CN weight - CN DiskSpace
Where,
CN weight --Container Weight
CN DiskSpace --Container disk space
CN Avail --Container Available
Step 1 : Select object storage.
Step 2 : Select container in object storage.
Step 3 : check availability in container.
CN Avail = CN weight - CN DiskSpace
Step 4 : check weight of container.
CN weight = CN DiskSpace + CN Avail
Step 5 : Store the files in container.

2) Partition for text file

Step 1 : Browse the File for Partition.
Step 2 : Set no of lines to split.
Step 3 : Set count to find no of lines in the file.
Step 4 : Partitioning File:
Split = Count / No of lines.

Step 5 : Set new files.
New files = Split.
Step 6 : Create output path.
Step 7 : Show newly generated file in output path.

3) Partition for Image file

Step 1 : Browse the image for Partition.
Step 2 : Set rows and columns for split the image.
Step 3 : Give value to rows and columns.
Step 4 : Set chunks to calculate rows and columns.
Chunks = rows * columns.
Step 5 : Set chunk Width and chunkHeight to determine the chunk size.
Step 6 : Set count to find no of chunks.
Count = Chunks.
Step 7 : Create output path.
Step 8 : Show newly generated images in output path.

4) Merge for text file

Step 1 : Browse the File for merge.
Step 2 : Create output path.
Step 3 : Set files to find no of splitted files.
Step 4 : Set mergedfile to store output path.
Step 5 : Set aLine to find no of lines in each file.
Step 6 : Merging File:
Merge = files + aLine.
Step 7 : Show newly generated file in output path.

5) Merge for Image file

Step 1 : Browse the image for Partition.
Step 2 : Set rows and columns for merge the image.
Step 3 : Set chunks to calculate rows and columns.
Chunks = rows * columns.
Step 4 : Set chunkWidth and chunkHeight to determine the chunk size.
Step 5 : Set finalImg to create output image.
Step 6 : finalImg = chunkWidth*columns + chunkHeight*rows.
Step 7 : Create output path.
Step 8 : Show newly generated images in output path.

V. CONCLUSION

The conclusion of the paper shows that the software and information has been provided to computers which are described as a service rather than a product. As a single server that handles the multiple requests from the user, the delay in data management of loss of data and packet management is reduced by applying the proposed algorithm (biometric authentication) of the paper. The data storage on un-trusted cloud makes as a security issue. Data security in the cloud is guaranteed by the privacy of delicate information should be enforced on Cloud storage. Also reduces users botheration about losing control of their own data. As a whole the author tested the data with SVM techniques using UCI repository. This has fetched efficient and effective outcome by the proposed model. Finally, to store the data through data placement algorithm, to provide authentication and secure access control for data using Crypto-Biometric System (CBS) in cloud computing and to protect the data from unauthorized access has been made.

VI. ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the editor-in-chief of the journal for their valuable guidance which

has improved the quality and presentation of the paper.

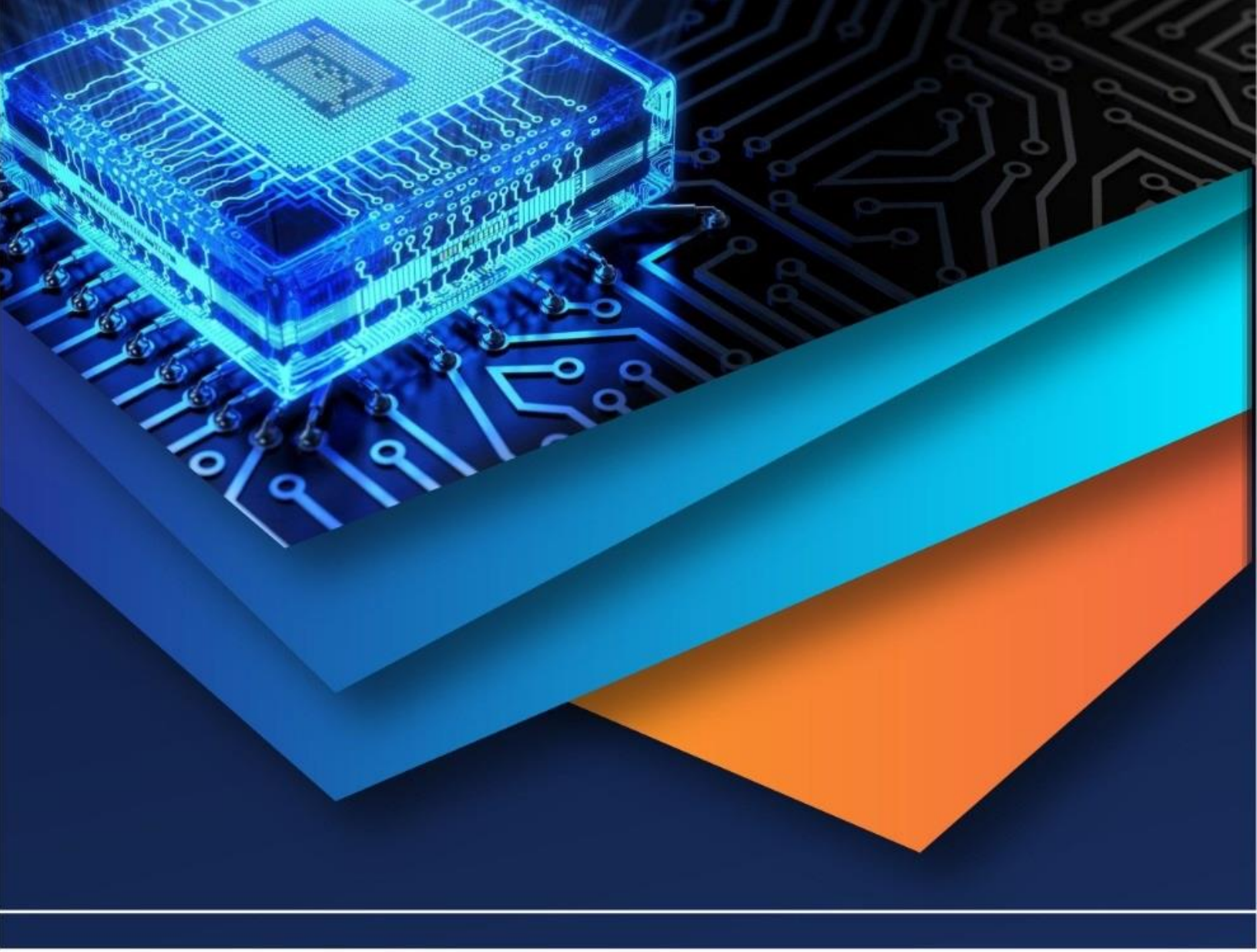
REFERENCES

[1] Meenakshi et.al., Data security analysis in cloud environment, International journal of innovations & advancement in computer science vol.2(1),pp.14-19,2014.
[2] Prashant rewagad and yogar , Use of digital signature with Diffie Hellman key Exchange and AES encryption algorithm to enhanced data security in cloud computing, International Journal of Scientific and Research Publications, vol.3(13),pp.437-439,June 2015.
[3] Prasanthi and Subba , Enhanced AES Algorithm, International Journal of Computer Applications in Engineering Sciences, vol 2 (2),pp.114-118,June 2012.
[4] T.Sivasakthi, and N Prabakaran, Applying Digital signature with Encryption Algorithm of user Authentication for Data Security in cloud computing, IJIRCCE, vol 2,2014.
[5] Subhas Barman, Samiran Chattopadhyay Debasis Samanta, An Approach to cryptographic key Exchange using Fingerprint, Springer-Verlag Berlin Heidelberg 2014.
[6] Abdullah A.Albahdal , Terrance E.Boult, Problems and promises of using the cloud and biometrics, 11th ICIT,2014.
[7] Kuyoro S.O, Lbikunle F, Awodele O, Cloud computing Security Issues and challenges, International Journal of Computer Science and Information Technology & Security, vol-3.2011.
[8] K.S.Suresh, K.V.Prasad, Security Issues and security algorithms in cloud computing, International Journal of Advanced Research in Computer Science and Software Engineering, vol-2,October, 2012.
[9] Jasim, Omer K., and Safia Abbas, Efficiency of Modern Encryption Algorithms in cloud computing, International Journal of Emerging Trends & Technology in Computer Science , 2.6, December, 2013: 270-274.
[10] Khanna, Leena, and Anant Jaiswal, Cloud computing :security Issues and description of encryption based algorithms to overcome them, International Journal of Advanced Research in Computer Science and Software Engineering 3.3 pp.nos. 279-283,March, 2013.
[11] Abha, Mohit, and Mohit Bhansali, Enhancing cloud computing security using AES Algorithm, International Journal of Computer Applications pp.nos.67.9 ,2013.
[12] Kalpana, Parsi, and Sudha Singaraju, Data security in cloud computing using RSA algorithm, International Journal of Research in Computer and Communication Technology 1.4 ,pp.nos.143-146,2012.
[13] Sawdekar, Poonam, and Seema Shah, Implementation of Information Leakage Avoiding (ILA) Application in Cloud Computing , International Journal of Computer Applications pp.nos.97.13, July,2014.
[14] IBM Corporation, IBM Bluemix [Online] Available https //www bluemix net/
[15] Tiancheng Li; Ninghui Li; Jian Zhang; Molloy, I.,Slicing: A New Approach for Privacy Preserving Data Publishing, Knowledge and Data Engineering, IEEE Transactions on, vol.24, no.3, pp.561-574,2012.

AUTHORS PROFILE

Prabu S have completed his Bachelor of Engineering in Computer Science and Engineering from Sona College of Technology Salem and Master of Technology in Information Technology from School of Computer Science and Engineering, Bharathidasan University Trichy. His research interest is Data Security in Cloud Environment.

Dr. Gopinath Ganapathy is Professor and Chair School of Computer Science, Engineering and Applications, Bharathidasan University,Tiruchirappalli, Tamil Nadu, India. He has more than 35 publications in national and international journals and conferences. He organized many Conferences which includes one IEEE Conference as chair and also participated in many workshops and seminars. He is a member of many professional bodies. His area of interest Software Development Business Analysis Cloud Computing, Software Project Management, Project Management,Enterprise Architecture.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY