ISSN:2231-0711

Prabu S et al | IJCSET(www.ijcset.net) | 2017 | Volume 7, 10-14

Secured Data Storage in public Cloud Environment through Crypto-Biometric System

Prabu S[#1], Gopinath Ganapathy[#2]

[#]*School of Computer Science, Engineering and Applications, Bharathidasan University Tiruchirappalli 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 obfuscated 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 obfuscated 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 was 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. RELATED WORKS

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.

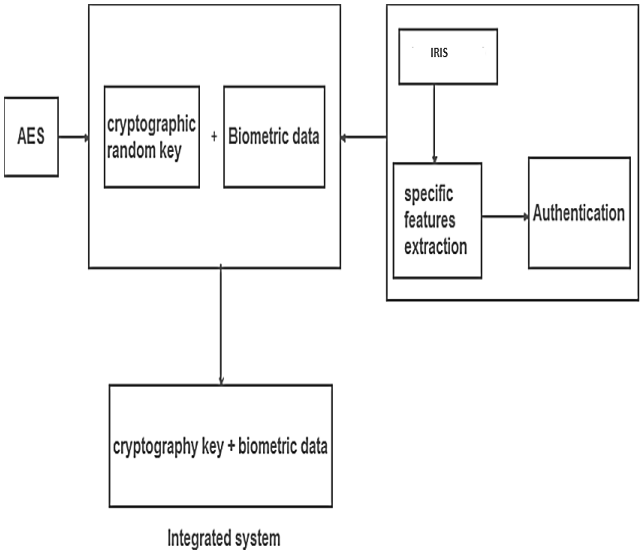

Fig.1 Crypto-Biometric System model

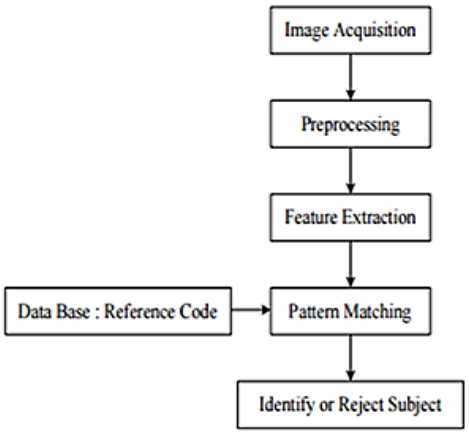

Fig.2 Phases of IRIS Recognition

The figure 2 discuss about the Iris Recognition. A few hundred a large number of persons in a few nations around the globe have been selected in iris recognition frameworks for comfort purposes, for example, travel permit free robotized fringe intersections, and some national ID programs. A key favourable position of iris recognition, other than its rate of coordinating and its compelling imperviousness to false matches, is the security of the iris as an inner and ensured, yet remotely unmistakable organ of the eye.

A. Image Acquisition

An image of the eye to be investigated must be gained first in advanced structure appropriate for examination.

B. Image Pre-processing

1. Algorithm for detection and segmentation

Iris recognition Irises is distinguished notwithstanding when the images have checks, visual clamour and diverse levels of brightening. Lighting reflections, eyelids and eyelashes checks are killed. Images with limited eyelids or eyes that are looking endlessly are additionally acknowledged utilizing wavelet calculation.

2. Programmed intertwining location and adjustment

The revision results in greatest nature of iris components layouts from moving iris images. Looking without end eyes: A looking ceaselessly iris image is accurately identified, portioned and changed as though it were looking specifically into the camera.

Right iris division is accomplished under these conditions: Immaculate circles fizzle. VeriEye utilizes dynamic shape models that all the more precisely model the forms of the eye, as flawless circles don't display iris limits. The focuses of the iris internal and external limits are distinctive. The iris inward limit and its middle are set apart in red; the iris external limit and its inside are set apart in green. Iris limits are unquestionably not circles and even not ovals and particularly in looking endlessly iris images. Iris limits appear to be immaculate circles. The recognition quality can even now be enhanced if limits are discovered more precisely on comparison with impeccable round white forms.

To find Iris, the main processing step comprises of in finding the internal and external limits of the iris and second means to standardize iris and third means to upgrade the first image].The Daugman's framework, Integro differential administrators as in is utilized to distinguish the inside and width of iris and understudy individually. The modules are used in this are

- Architecture Optimization
- Filter Optimization
- Elementary Pre-processing
- Evaluation Protocol

3. Architecture Optimization

Thinking of one as layer and conceivable estimations of each hyper parameter, there are more than 3,000 conceivable layer architectures, and this number becomes exponentially with the quantity of layers, which goes up to three for our situation. Furthermore, there are system level hyper parameters, for example, the measure of the info image, that extend conceivable outcomes to heap potential architectures. The general arrangement of conceivable hyper parameter qualities is called seek space, which for this situation is discrete and contains variables that are just important in mix with others. For instance, hyper parameters of a given layer are simply significant if the applicant architecture has really that number of layers. Notwithstanding the inborn trouble in improving architectures in this space, arbitrary hunt has assumed and critical part in problems of this write and it is our preferred technique because of its viability and effortlessness.

4. Filter Optimization

For streamlining filters, there is a need of an officially characterized architecture. The paper begins with the streamlining filters with a standard open convolutional system and preparing strategy. This system is accessible in the CUDA-convent library and is at present one of the best performing architectures in CIFAR-10,3 a mainstream PC vision benchmark in which such system accomplishes 11% of characterization mistake. Hereinafter, there is a need to call this system cuda-convnet-cifar10-11pct, or just cf10-11. Ten preparing tests are produced from a solitary image.

5. Elementary Pre-processing

A couple of fundamental pre-processing operations were executed on iris and retinal images with a specific end goal to legitimately learn representations for these benchmarks. This pre-processing prompted images with sizes as presented in Table II and are depicted in the following two areas.

IRIS images: Given that the face benchmarks considered in this work are video-based, firstly, equal subsample 10 outlines from every information video. At that point, the paper distinguishes the retinal position utilizing Viola and Jones and yield a region of 200 × 200 pixels focused at the identified window.

Retinal Images: Given the various ways of images caught from various sensors, here the pre-processing is characterized by sensor sort.

Biometrical: The trimming of the focal region of size in sections and lines relating to 70% of the first image measurements is made.

Italdata and Cross Match: The paper deals with the focal region of size in segments and lines separately relating to 60% and 90% of the first image segments and columns.

Swipe: As the images procured by this sensor contain a variable number of clear columns at the base, the normal

number of non-clear lines M was initially ascertained from the preparation images. At long last, the edition of the focal region relating to 90% of unique image segments and M columns.

6. *Evaluation Protocol*

The paper deals with the standard evaluation protocol of all benchmarks and assess the strategies as far as location precision (ACC) and half aggregate mistake rate (HTER), as these are the measurements used to survey progress in the arrangement of benchmarks considered thus. Precisely, for a given benchmark and convolutional organize effectively prepared, results are acquired by:

- Retrieving prediction scores from the testing tests;
- Calculating an edge τ above which tests are predicted as assaults;
- Computing ACC and/or HTER utilizing τ and test predictions.

Algorithms utilized are Local Difference Probability (LDP)- Based Environment Adaptive Algorithm and Histogram of Oriented-inclinations.

Matching

In the matching step, a score that indicates the similarity between two iris images is performed.

IRIS Recognition

IRIS recognition is a mechanized strategy for biometric identification that utilizations scientific example recognition procedures on images of either of the irises of an individual's eyes, whose mind boggling irregular examples are special, stable, and can be seen from some separation.

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 maintaining 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 is an 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.

IV.ALGORITHM

A. *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.

B. *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.

C. *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.

D. *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.

E. 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.

IV. CONCLUSIONS

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.

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] Thapliyal, Meenakshi, Hardwari Lal Mandoria, and Neha Garg. “Data security analysis in cloud environment”, International journal of innovations and 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, 2015.
[3] Prasanthi and Subba, “Enhanced AES Algorithm”, International Journal of Computer Applications in Engineering Sciences, Vol 2 (2), pp.114-118, 2012.
[4] T.Sivasakthi, and N Prabakaran, “Applying Digital signature with Encryption Algorithm of user Authentication for Data Security in cloud computing”, International Journal of Innovative Research in Computer and Communication Engineering, Vol 2(2), pp. 456-459,2014.
[5] Barman, Subhas, Samiran Chattopadhyay, and Debasis Samanta. "An approach to cryptographic key exchange using fingerprint." International Symposium on Security in Computing and Communication. Springer Berlin Heidelberg pp.162-172, 2014.
[6] Albahdal, Abdullah A., and Terrance E. Boult. "Problems and Promises of Using the Cloud and Biometrics." Information Technology: New Generations (ITNG), 2014 11th International Conference on. IEEE, pp. 293-300, 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, 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, Vol.2(6),pp. 270-274, 2013.
[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, Vol.3(3), pp. 279-283, 2013.
[11] Abha, Mohit, and Mohit Bhansali, Enhancing cloud computing security using AES Algorithm, International Journal of Computer Applications, pp.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, Vol.1(4), pp.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.7-13, 2014.
[14] IBM Corporation, IBM Bluemix [Online] Available https //www bluemix net/
[15] Tiancheng Li; Ninghui Li; Jian Zhang; Molloy, I.,Slicing: “Slicing: A new approach for privacy preserving data publishing”, IEEE transactions on knowledge and data engineering, Vol.24(3), pp.561-574,2012.