



# Designing Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services

SANDHYA GANDI <sup>#1</sup>, VARDU RAJASEKHAR <sup>#2</sup>

<sup>#1</sup> Assistant Professor, Department of Computer Science and Engineering,  
Sanketika Vidhya Parishad Engineering College, P.M. Palem,  
Visakhapatnam, Andhra Pradesh.

<sup>#2</sup> MCA Student, Department of Computer Science and Application,  
Sanketika Vidhya Parishad Engineering College, P.M. Palem,  
Visakhapatnam, Andhra Pradesh.

## ABSTRACT

In current days cloud computing is providing great flexibility for the end-users to store and access a lot of valuable information to and from remote servers. As we all know that data is uploaded into the cloud is outsourced to a third party untrusted remote server, privacy for that data is almost a big problem for the enterprises. Hence in this current project, we try to add a new level of security for the cloud data by adding biometric authentication techniques like fingerprint images and then verify the user authentication based on the biometric images. Here we try to design a mutual authentication scheme based on bio-metric based secure access scheme for cloud computing to avoid the illegal data access by unauthorized users and in which this will be divided into two phases for providing security. In first phase the user is asked to choose bio metric authentication in the form of finger print images and in the second phase the owner can upload bio metric related data into the cloud server in a secure manner by encrypting the files using cryptography algorithms.

## KEYWORDS:

Cloud Computing, Biometric Authentication, Finger Print Images, Remote Servers, Cryptography, Encryption.

## 1. INTRODUCTION

Biometric Authentication System gives a huge number of virtual and intensely flexible resources, for instance, handling resources, accumulating, gear stages and applications to customers by methods for Internet. This gives customers a great deal of flexibility and convenience. Further, customers can store such a data into cloud and the proportionate can be gotten to at whatever point and from wherever by methods for Internet. Regardless, conveyed registering in like manner brings extraordinary security issues, especially for customers' data set aside in the cloud[1]. At the point when the data is re-appropriated to a pariah, the data security has become a critical issue, including the issue of which the unlawful customers get to

the benefit of cloud specialist to take data of genuine customers and the legitimate customers get to the illegal labourer. To make sure about customers' assurance, when the legal cloud customers get the chance to cloud organization resources, customers need to check the cloud labourer, and cloud specialist needs to perceive the customers' login sales to ensure that the customers are genuine customers[2]-[7].

In this manner, many light weight customer check shows had been proposed. There are three fundamental check ways: Password based approval, Biometric-based affirmation, and Biometric-based approval. Since mystery key based approval is unprecedented insecurity, and the cost of biometrics-based check plot is higher and for the most part sensible for a raised degree of characterization, the Biometric-based affirmation has been proposed for its advantage and sound judgment. L.Lamport first proposed an approval plot in the open channel [8]. Starting now and into the foreseeable future, Hwang and Li proposed an ElGamal cryptosystem based Biometric approval plot. In any case, it has been shown that Hwang and Li's arrangement can't maintain a strategic distance from emulate attacks[9]. Song[10] proposed another Biometric affirmation plot. He attested that the arrangement can restrict the current likely attacks. Additionally, it achieves normal affirmation and gives shared gathering key. However, it is shown that Song's arrangement is powerless against DOS ambushes. Starting late, Singhal et al.[11] presented a mutual affirmation plot. Makers ensured that their arrangement is secure against lost Biometric ambush, detached mystery word hypothesizing attack, camouflage ambush and replay ambush. Further, the arrangement gives normal affirmation and secure gathering key age.

Regardless, it is exposed against lost Biometric ambush and detached mystery key guessing attack. In order to beat these

obstructions, redesigned cloud shared check plan is proposed in this paper. The proposed scheme relies upon Singhal et al's. Plot using hash limits. Execution assessment shows that the proposed plot is a profitable one

## 2. LITERATURE SURVEY

Literature survey is that the most vital step in software development process. Before developing the new application or model, it's necessary to work out the time factor, economy and company strength. Once all these factors are confirmed and got an approval then we can start building the application. The literature survey is one which is mainly deal with all the previous work which is done by several users and what are the advantages and limitations in those previous models. This literature survey is mainly used for identifying the list of resources to construct this proposed application.

### MOTIVATION

**BLACR: without ttpblacklistable obscure confirmations with reputation**

**Authors: M. H. Au, A. Kapadia, and W. Susilo**

Baffling approval can give customers the license to turn crazy since there is no fear of retaliation. As an obstacle, or means to refusal, various designs for mindful mystery feature a (possibly passed on) trusted in untouchable (TTP) with the capacity to recognize or interface misbehaving customers. Starting late, plans, for instance, BLAC and PEREA showed how obscure denial can be practiced without such TTPs—strange customers can be disavowed in case they get into wickedness, yet then nobody can recognize or association such customers cryptographically. Regardless of being the top tier in obscure revocation, these plans license only an essential sort of renouncement signifying 'deny anybody with d or more wicked exercises' or 'repudiate anybody whose joined wrongdoing score is unreasonably high'

(where devilish exercises are dispensed a 'reality' score). We present BLACR, which generally impels secretive forswearing in three unique manners:

1) It sets up a first undertaking to summarize reputation based obscure denial, where negative or positive scores can be delegated to strange gatherings over different classes. Laborers can square customers subject to methodologies, which decide a boolean mix of reputations in these orders; 2) We present a weighted expansion, which allows the full scale earnestness score to increment for different wicked exercises by a comparative customer; and, 3) We make an immense improvement in approval times through a strategy we call express way affirmation, which makes reputation based obscure renouncement sensible.

### **PERM: Practical reputation based boycotting without TTPS**

**Authors: M. H. Au and A. Kapadia**

A couple of customers may get into underhandedness under the front of anonymity by, e.g., harming site pages on Wikipedia or posting revolting comments on YouTube. To thwart such abuse, a few obscure accreditation plans have been proposed that repudiate access for getting into wickedness customers while keeping up their anonymity with the ultimate objective that no trusted in pariah (TTP) is locked in with the denial technique. Starting late we proposed BLACR, a without ttp plot that supports 'reputation based boycotting' - the pro community can score customers' strange gatherings (e.g., incredible versus ill-advised comments) and customers with lacking reputation are denied get to. The critical drawback of BLACR is the direct computational overhead in the size of the reputation list, which grants it to help reputation for only a few thousand customer gatherings in valuable settings. We propose PERM, a disavowal window-based arrangement (wicked exercises must be gotten inside a window of time), which makes count liberated from the size of the reputation list. PERM in this manner supports a considerable

number of customer gatherings and makes reputation based boycotting rational for gigantic extension courses of action.

### **Constant-size one of a kind k-TAA**

**Authors: M. H. Au, W. Susilo, and Y. Mu**

Dynamic k-times obscure confirmation (k-TAA) plans grant people from a social occasion to be affirmed subtly by application providers for a predetermined number of times, where application providers can self-rulingly and logically grant or deny get the opportunity to right to people in their own get-together. In this paper, we fabricate an incredible k-TAA plot with reality complexities of  $O(\log(k))$  and a variety, where the check show just requires consistent presence complexities to the detriment of  $O(k)$  - estimated open key. We in like manner portray some tradeoff issues between different system characteristics. We detail all the zero-data affirmation of-data shows included and show that our improvement is secure in the discretionary prophet model under the q-strong Diffie-Hellman assumption and q-decisional Diffie-Hellman inversion doubt. We give a proof-of-thought execution, test its display, and show that our arrangement is businesslike.

### **3. EXISTING SYSTEM AND ITS LIMITATIONS**

All the existing systems failed to provide security for the end users who try to store and access the sensitive information to and from the cloud servers. There is no concept of authenticating users based on bio metric image authentication and storing bio metric related data into application.

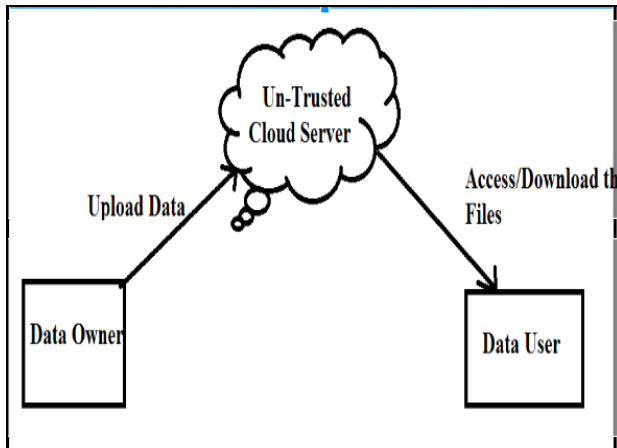
#### **LIMITATION OF PRIMITIVE SYSTEM**

The following are the limitations of the existing system.

1. Till now there was no method in cloud literature which can provide security for the outsourced data.

2. Almost all the cloud servers try to store the data in plain text manner rather than in encrypted manner.
3. The current cloud servers always authenticate the user account with the help of only username and password which will not provide more security for the enterprises for storing their data.

#### Existing Cloud Architecture



#### **4. PROPOSED SYSTEM AND ITS ADVANTAGES**

Hence in this current project, we try to add a new level of security for the cloud data by adding biometric authentication techniques like fingerprint images and then verify the user authentication based on the biometric images. Here we try to design a mutual authentication scheme based on bio-metric based secure access scheme for cloud computing to avoid the illegal data access by unauthorized users and in which this will be divided into two phases for providing security.

##### **ADVANTAGES OF THE PROPOSED SYSTEM**

1. The data is secure in this proposed method.
2. All the outsource data will be encrypted and then stored into the cloud server
3. The data can be accessed only by the authorized users rather than all users
4. The data can be authenticated by using the bio metric authentication like finger prints.

#### **5. IMPLEMENTATION PHASE**

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My SQL data base. The application is divided mainly into following 4 modules. They are as follows:

##### **1) DATA OWNER MODULE**

In this module, the data owner uploads their Biometric images with their contents data to the Cloud server. For the security purpose the data owner assigns the digital sign and then store in the Cloud and also performs the following operations such as Upload Biometric image with its digital sign based on title, desc, List all uploaded Biometric images, Verify Biometric image details, and Delete Biometric image details

##### **2) CLOUD SERVER MODULE**

The Cloud service provider manages a Cloud to provide data storage service. And performs the following operations such as Store all Biometric image files with their signature, View all Biometric image Files with its details, View all Biometric image comments, View all Data owners and Users, and View all attackers

##### **3) END USERS MODULE**

The Cloud User who has a large amount of data to be stored in Cloud Servers and have the permissions to access and manipulate stored Biometric image and its data. The consumer will search the data and

accessing the Biometric image data if he is authorized and performs the following operations such as Search Biometric image , Access Biometric image and its details, Download Biometric image & make comments

### 6. EXPERIMENTAL RESULTS

In this section we try to design our current model using Java as programming language and taking MY-SQL as storage database. Here the front end of the application is designed using JSP and HTML and back end we used My-SQL server.Now we can check the performance of our proposed application as follows:

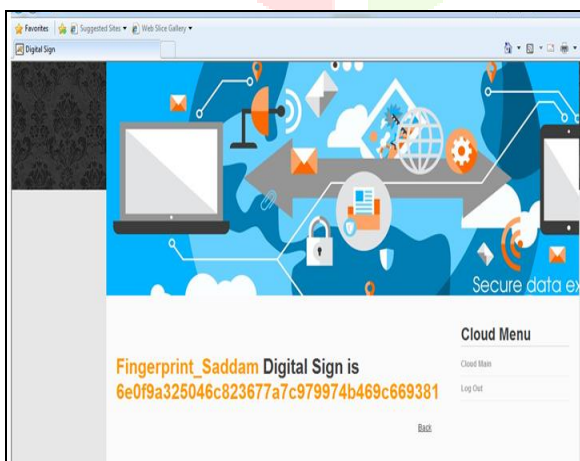
#### Cloud Server Views all the Bio Metric Files

View All Owner Bio Image Files

Arjun Uploaded Image Details

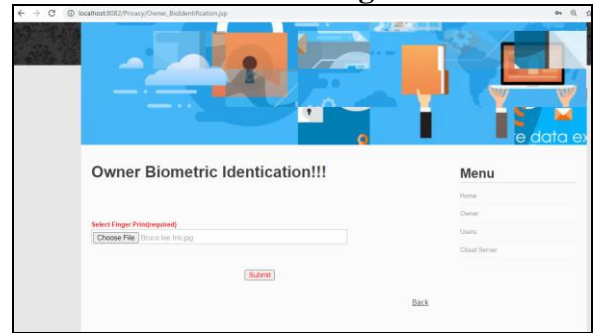
Image	Title	Name	Secret Key	Date	Rank	Digital Sign
	Iris	Bruceleece_Iris	[B@16b61c3	09/10/2018 12:55:36	2	View
	Iris1	Osama_Bin_laden_Iris	[B@73a5d3	09/10/2018 13:01:24	0	View

#### Data User/Owner Choose Fingerprint

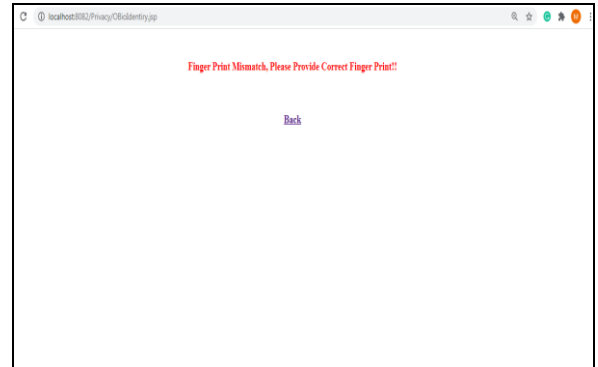


Fingerprint\_Saddam Digital Sign is  
6e0f9a325046c823677a7c979974b469c669381

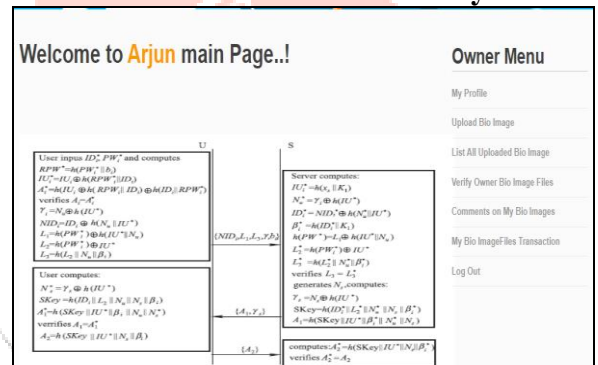
### Owner/User need to Authenticate with Bio Metric Images



#### If Bio Metric Mismatches



#### If Bio Metric Matches Successfully



### 7. CONCLUSION

In this paper, we for the first time designed a model to add a new level of security for the cloud data by adding biometric authentication techniques like fingerprint images and then verify the user authentication based on the biometric images. Here we try to design a mutual authentication scheme based on a smartcard for cloud computing to avoid the illegal data access by unauthorized users and in which this will be divided into two phases for providing security. By conducting various experiments on our proposed method we finally came to an conclusion that our proposed method of smartcard authentication system can able to give high level of security for the users

who try to access the sensitive information like iris related data in a secure manner and we can also able to restrict the un-authorized users not to enter the others account and try to view the data illegally.

## REFERENCES

[1] D. Zissis and D. Lekkas, “Addressing cloud computing security issues”, *Future Generation Computer Systems*, Vol.28, No.3, pp.583–592, 2012.

[2] F. Wen, X. Li and S. Cui, “An improved dos-resistant id-based password authentication scheme without using smartcar”, *Journal of Electronics (China)*, Vol.28, No.4, pp.580–586, 2011.

[3] K. Fan, J. Li, H. Li, *et al.*, “RSEL: Revocable secure efficient lightweight RFID authentication scheme”, *Concurrency and Computation: Practice and Experience*, Vol.26, No.5, pp.1084–1096, 2014.

[4] K. Fan, Y. Gong, Ch. Liang, *et al.*, “Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G”, *Security and Communication Network*, Wiley Online Library, DOI: 10.1002/sec.1314, 2015.

[5] C.D. Jaidhar, “Enhanced mutual authentication scheme for cloud architecture”, *3rd International Advance Computing Conference*, pp.70–75, 2013.

[6] M. Sarvabhatla and C.S. Vorugunti, “A robust mutual authentication scheme for data security in cloud architecture”, *Future Information Security Workshop COMSNETS*, pp.1–6, 2015.

[7] L. Lamport, “Password authentication with insecure communication”, *Communications of the ACM*, Vol.24, No.11, pp.770–772, 1981.

[8] M.S. Hwang and L.H. Li, “A new remote user authentication scheme using smartcards”, *IEEE Transactions on Consumer Electronics*, Vol.46, No.1, pp.28–30, 2000.

[9] C.K. Chan and L.M. Cheng, “Cryptanalysis of a remote user authentication scheme using smartcards”, *IEEE Transactions on Consumer Electronics*, Vol.46, No.4, pp.992–993, 2000.

[10] R. Song, “Advanced smartcard based password authentication protocol”, *Computer Standards Interfaces*, Vol.32, No.5–6, pp.321–325, 2010.

[11] A. Singhal and M. Ramaiya, “A novel safe and efficient smartcard authentication scheme using hash function”, *Engineering Universe for Scientific Research and Management*, Vol.7, No.1, pp.1–6, 2015.

[12] T.S. Messerges, E.A. Dabbish and R.H. Sloan, “Examining smartcard security under the threat of power analysis attacks”, *IEEE Transactions on Computers*, Vol.5, No.3, pp.514–522, 2002.

## About the Authors



**SANDHYA GANDI** is currently working as an Assistant Professor in Department of Computer Science and Engineering at Sanketika Vidhya Parishad Engineering College, P.M. Palem, Visakhapatnam, Andhra Pradesh. She has more than 10 years of teaching experience. Her research interest includes

Java, Python, .Net, HTML.



**VARDU RAJASEKHAR** is currently pursuing his 2 years MCA in Department of Computer Science and Applications at Sanketika Vidhya Parishad Engineering College, P.M. Palem, Visakhapatnam, Andhra Pradesh. His area of interest includes C, C++, Java and Python.