

A NOVEL METHOD TO PROTECT THE PRIVACY OF CLOUD DATA USING SMARTCARD AUTHENTICATION

BONDA DIVYA PRASANTHI ^{#1}, K.RAMBABU ^{#2}

^{#1} MCA Student, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

^{#2} Head & Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

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 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.

Keywords: Cloud Computing, Smart Card Authentication, Encryption, Decryption

1. INTRODUCTION

Cloud computing provides a large number of virtual and dynamically scalable resources, such as computing resources, storage, hardware platforms and applications to users via Internet. This provides users with a great deal of flexibility and convenience [1]. Further, users can store any kind of data into cloud and the same can be accessed at any time and from anywhere via Internet. However, cloud computing also brings very serious security problems, especially for users' data stored in the cloud.

Once the data is outsourced to a third party, the data privacy has become a major problem, including the problem of which the illegal users access the resource of cloud server to steal data of legal users and the legal users access the illegal server. In order to protect users' privacy, when the legal cloud users access cloud service resources, users need to verify the cloud server, and cloud server needs to identify the users' login requests to ensure that the users are legal users. As a result, many light weight user authentication protocols had been proposed[2–6]. There are three basic authentication ways: Password based authentication, Smartcard-based authentication, and Biometric-based authentication.

Because password based authentication is great insecurity, and the cost of biometrics-based authentication scheme is higher and most suitable for a high level of confidentiality, the smartcard-based authentication has been proposed for its convenience and practicality. L.Lamport first proposed an authentication scheme in the open channel[7]. Since then, Hwang and Li[8] proposed an ElGamal cryptosystem based smartcard authentication scheme. However, it has been demonstrated that Hwang and Li's scheme cannot resist impersonation attacks[9]. Song[10] proposed a new smartcard authentication scheme. He claimed that the scheme can resist the existing potential attacks. In addition, it achieves mutual authentication and provides shared session key. But it is shown that Song's scheme is vulnerable to DOS attacks. Recently, Singhal *et al.*[11] presented a mutual authentication scheme. Authors claimed that their scheme is secure against lost smartcard attack, offline password guessing attack, masquerade attack and replay attack. Further, the scheme provides mutual authentication and secure session key generation.

However, it is vulnerable to lost smartcard attack and offline password guessing attack. In order to overcome these limitations, enhanced cloud mutual authentication scheme is proposed in this paper. The proposed scheme is based on Singhal *et al.*'s scheme using hash functions. Performance comparison shows that the proposed scheme is an efficient one. 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. This is providing users with a lot of new features for accessing and storing the information in a more flexible manner with great convenience. Since it is having a lot of advantages and security still it has some security problems like it is not providing security for enterprise data security. 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.

2. LITERATURE SURVEY

Cloud computing is the utilization of processing assets (equipment and programming) that are conveyed as an administration over a system (normally the Internet). The name originates from the regular utilization of a cloud-formed image as a deliberation for the perplexing foundation it contains in framework outlines. Distributed computing endows remote administrations with a client's information, programming and calculation. Distributed computing comprises of equipment and programming assets made accessible on the Internet as oversaw outsider administrations. These administrations regularly give access to cutting edge programming applications and top of the line systems of server PCs.

RELATED WORK

1) PERM: Practical reputation-based blacklisting without TTPS

AUTHORS: M. H. Au and A. Kapadia

Some users may misbehave under the cover of anonymity by, e.g., defacing webpages on Wikipedia or posting vulgar comments on YouTube. To prevent such abuse, a few anonymous credential schemes have been proposed that revoke access for misbehaving users while maintaining their anonymity such that no trusted third party (TTP) is involved in the revocation process. Recently we proposed BLACR, a TTP-free scheme that supports 'reputation-based blacklisting' --- the service provider can score users' anonymous sessions (e.g., good vs. inappropriate comments) and users with insufficient reputation are denied access.

The major drawback of BLACR is the linear computational overhead in the size of the reputation list, which allows it to support reputation for only a few thousand user sessions in practical settings. We propose PERM, a revocation-window-based scheme (misbehaviors must be caught within a window of time), which makes computation independent of the size of the reputation list. PERM thus supports millions of user sessions and makes reputation-based blacklisting practical for large-scale deployments.

2) BLACR: TTP-free blacklistable anonymous credentials with reputation

AUTHORS: M. H. Au, A. Kapadia, and W. Susilo

Anonymous authentication can give users the license to misbehave since there is no fear of retribution. As a deterrent, or means to revocation, various schemes for accountable anonymity feature some kind of (possibly distributed) trusted third party (TTP) with the power to identify or link misbehaving users. Recently, schemes such as BLAC and PEREA showed how anonymous revocation can be achieved without such TTPs—anonymous users can be revoked if they misbehave, and yet nobody can identify or link such users cryptographically. Despite being the state of the art in anonymous revocation, these schemes allow only a basic form of revocation amounting to 'revoke anybody with d or more misbehaviors' or 'revoke anybody whose combined misbehavior score is too high' (where misbehaviors are assigned a 'severity' score). We present BLACR, which significantly advances anonymous revocation in three ways: 1) It constitutes a first attempt to

generalize reputation-based anonymous revocation, where negative or positive scores can be assigned to anonymous sessions across multiple categories. Servers can block users based on policies, which specify a boolean combination of reputations in these categories; 2) We present a weighted extension, which allows the total severity score to ramp up for multiple misbehaviors by the same user; and, 3) We make a significant improvement in authentication times through a technique we call express lane authentication, which makes reputation-based anonymous revocation practical.

3) Constant-size dynamic k -TAA

AUTHORS: M. H. Au, W. Susilo, and Y. Mu

Dynamic k -times anonymous authentication (k -TAA) schemes allow members of a group to be authenticated anonymously by application providers for a bounded number of times, where application providers can independently and dynamically grant or revoke access right to members in their own group. In this paper, we construct a dynamic k -TAA scheme with space and time complexities of $O(\log(k))$ and a variant, in which the authentication protocol only requires constant time and space complexities at the cost of $O(k)$ - sized public key. We also describe some tradeoff issues between different system characteristics. We detail all the zero-knowledge proof-of-knowledge protocols involved and show that our construction is secure in the random oracle model under the q -strong Diffie–Hellman assumption and q -decisional Diffie–Hellman inversion assumption. We provide a proof-of-concept implementation, experiment on its performance, and show that our scheme is practical.

4) A secure cloud computing based framework for big data information management of smart grid

AUTHORS: J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang

Smart grid is a technological innovation that improves efficiency, reliability, economics, and sustainability of electricity services. It plays a crucial role in modern energy infrastructure. The main challenges of smart grids, however, are how to manage different types of front-end intelligent devices such as power assets and smart meters efficiently; and how to process a huge amount of data received from these devices. Cloud computing, a technology that provides computational resources on demands, is a good candidate to address these challenges since it has several good properties such as energy saving, cost saving, agility, scalability, and flexibility. In this paper, we propose a secure cloud computing based framework for big data information management in smart grids, which we call “Smart-Frame.” The main idea of our framework is to build a hierarchical structure of cloud computing centers to provide different types of computing services for information management and big data analysis. In addition to this structural framework, we present a security solution based on identity-based encryption, signature and proxy re-encryption to address critical security issues of the proposed framework

3. EXISTING SYSTEM

In the existing system a well-known authors L.Lamport have proposed an authentication scheme in the open channel. But the system is not up to the mark in providing security for the sensitive data from enterprises. Later another well-known author, Hwang and Li[8] proposed an ElGamal cryptosystem based smartcard authentication scheme ,but this scheme cannot resist impersonation attacks[9].Hence 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.

LIMITATION OF EXISTING 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.

4. PROPOSED SYSTEM

A mutual authentication scheme based on smartcard for cloud computing is proposed to solve the problem of which the illegal users access the resource of cloud servers and the legal users access the illegal cloud server. The scheme achieves mutual authentication by using hash functions to protect user privacy. Performance comparison shows that the proposed scheme is an efficient one.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the 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. SOFTWARE PROJECT MODULES

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. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed protocol. The application is divided mainly into following 3 modules. They are as follows:

1. Data Owner Module
2. Cloud Server Module
3. Data User Module

Now let us discuss about each and every module in detail as follows:

5.1 Data Owner

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

5.2 Cloud Server

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

5.3 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. OUTPUT RESULTS

USER CAN VIEW HIS SEARCH TRANSACTIONS

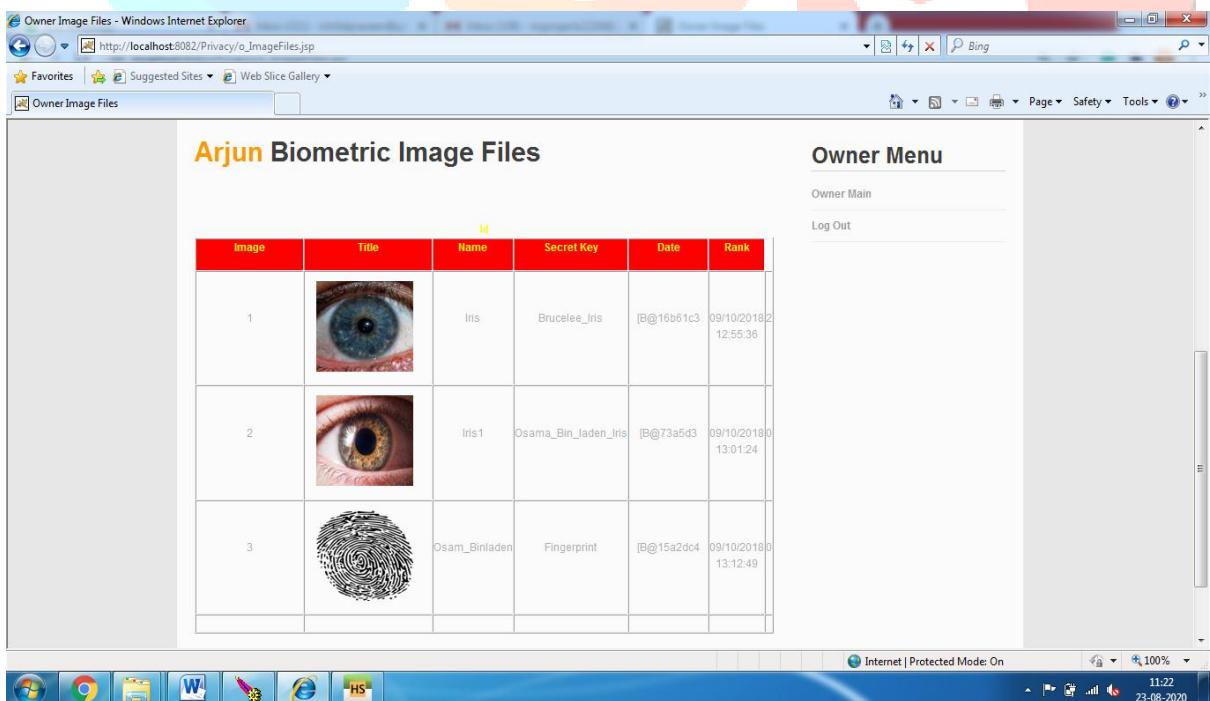


The screenshot shows a web browser window with multiple tabs open. The active tab displays a table titled "Comments on Arjun Biometric Images". The table has columns: SI NO, User Name, Image Name, SecretKey, Task, and Date. The data in the table is as follows:

SI NO	User Name	Image Name	SecretKey	Task	Date
1	My Upload	Brucelee_Iris	[B@16b61c3	Upload	09/10/2018 12:55:36
2	Amar	Brucelee_Iris	[B@16b61c3	Download	09/10/2018 12:57:21
4	Amar	Brucelee_Iris	[B@16b61c3	Download	09/10/2018 13:05:53
6	Amar	Brucelee_Iris	[B@16b61c3	Download	09/10/2018 13:06:48
10	tmksmanju	Brucelee_Iris	[B@16b61c3	Download	09/10/2018 16:13:54
13	tmksmanju	Brucelee_Iris	[B@16b61c3	Download	09/10/2018 16:16:48
3	My Upload	Osama_Bin_laden_Iris	[B@73a5d3	Upload	09/10/2018 13:01:24
5	Amar	Osama_Bin_laden_Iris	[B@73a5d3	Download	09/10/2018 13:05:58
7	My Upload	Fingerprint	[B@15a2dc4	Upload	09/10/2018 13:12:49

Below the table, there is a "Back" button. The browser's status bar at the bottom shows the date and time as 23-08-2020 11:21.

USER CAN VIEW THE LIST OF ALL BIO-METRIC IMAGES



The screenshot shows a web browser window with multiple tabs open. The active tab displays a table titled "Arjun Biometric Image Files". The table has columns: Image, Title, Name, Secret Key, Date, and Rank. The data in the table is as follows:

Image	Title	Name	Secret Key	Date	Rank
1		Iris	Brucelee_Iris	[B@16b61c3	09/10/2018 12:55:36
2		Iris1	Osama_Bin_laden_Iris	[B@73a5d3	09/10/2018 13:01:24
3		Osam_Binladen	Fingerprint	[B@15a2dc4	09/10/2018 13:12:49

On the right side of the screen, there is a sidebar titled "Owner Menu" with "Owner Main" and "Log Out" options. The browser's status bar at the bottom shows the date and time as 23-08-2020 11:22.

USER CAN VIEW HIS BIO METRIC IMAGES COMMENTS

Image Verification - Windows Internet Explorer

http://localhost:8082/Privacy/o_AllComments.jsp

Image Verification

Comments on Arjun Images

Commented By	Comments Details	Date
Amar	It is very useful	09/10/2018 12:57:43
tmksmanju	IT is useful in the crime activities	09/10/2018 16:14:26

Owner Menu

Owner Main

Log Out

ID	1
Image Title	Iris
Image Name	Bruceloo_Iris
Rank	2

ID	2
Image Title	Iris1
Image Name	Osama_Bin_Laden_Iris

Internet | Protected Mode: On

11:22 23-08-2020

USER LOGIN

(12) WhatsApp

Inbox (321) - mtsitdpriyaveen@gmail.com

Inbox (108) - myprojects2226@gmail.com

User Login Page

localhost:8082/Privacy/consumerLogin.jsp

Users Login Page..!

Menu

- Home
- Owner
- Users
- Cloud Server

User Name (required)

Amar

Password (required)

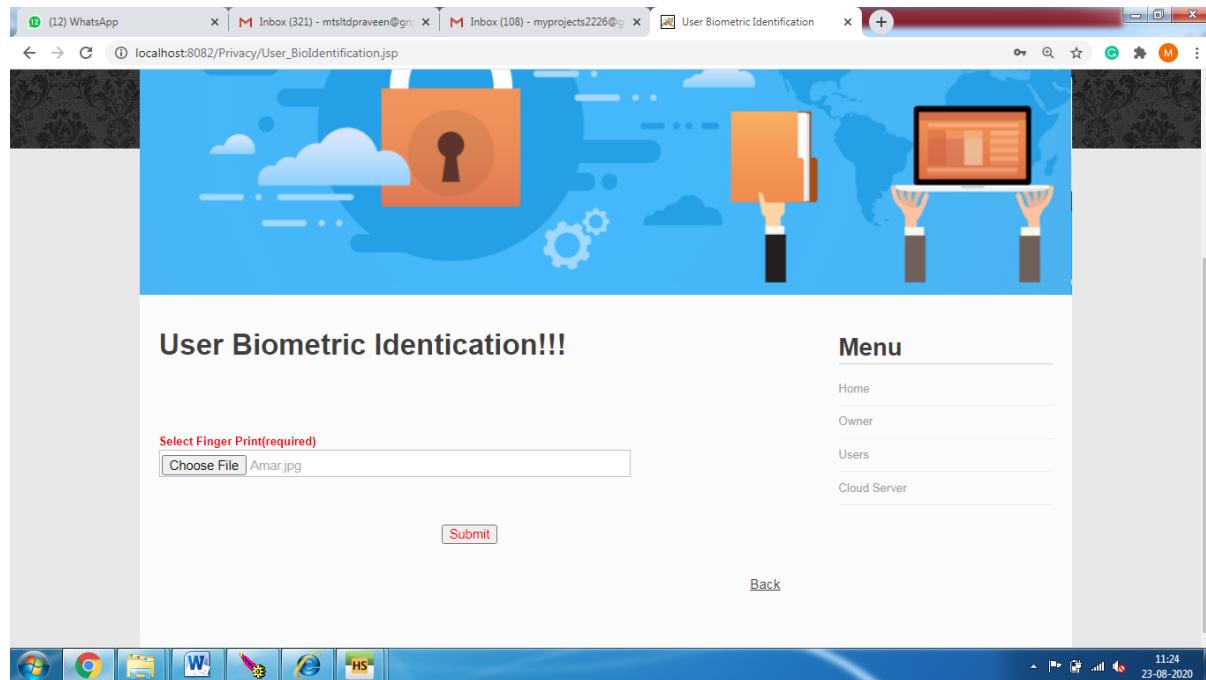
.....

Submit

Internet | Protected Mode: On

11:23 23-08-2020

USER HOME PAGE



User Biometric Identification!!!

Select Finger Print(required)

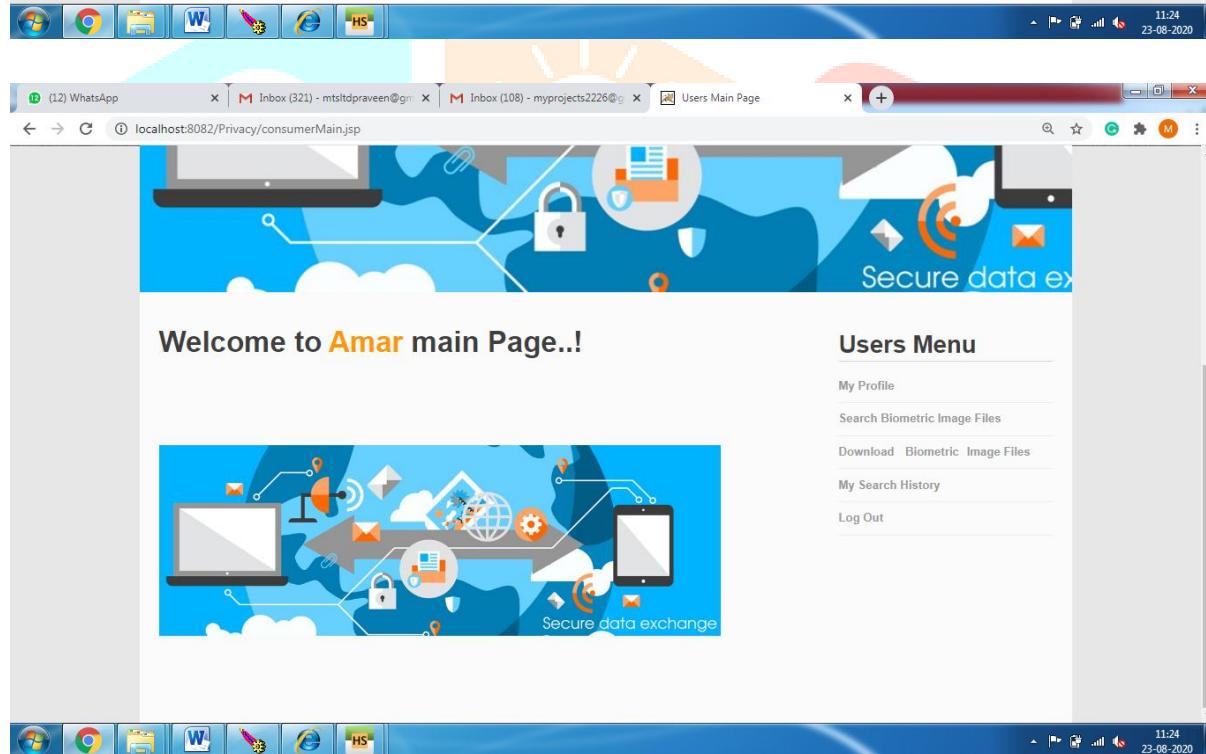
Choose File Amar.jpg

Submit

Back

Menu

- Home
- Owner
- Users
- Cloud Server



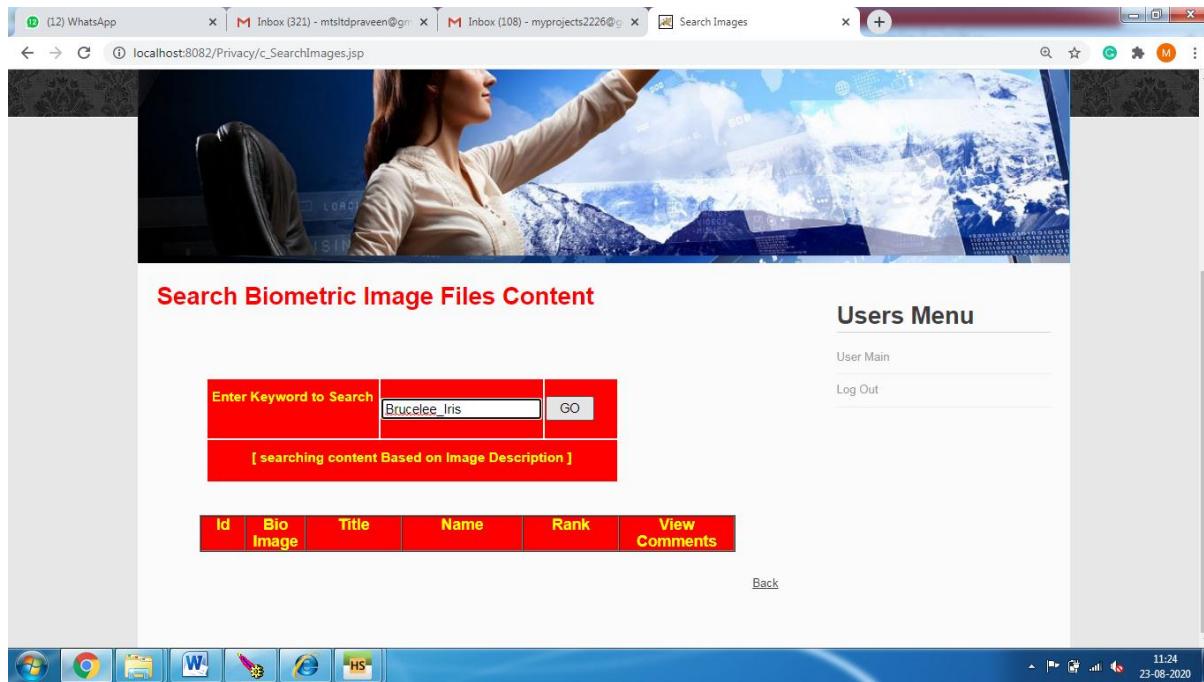
Welcome to Amar main Page..!

Secure data exchange

Users Menu

- My Profile
- Search Biometric Image Files
- Download Biometric Image Files
- My Search History
- Log Out

USER SEARCH BIO METRIC IMAGES



Search Biometric Image Files Content

Enter Keyword to Search: GO

[searching content Based on Image Description]

Id	Bio Image	Title	Name	Rank	View Comments
----	-----------	-------	------	------	---------------

[Back](#)

RESULT

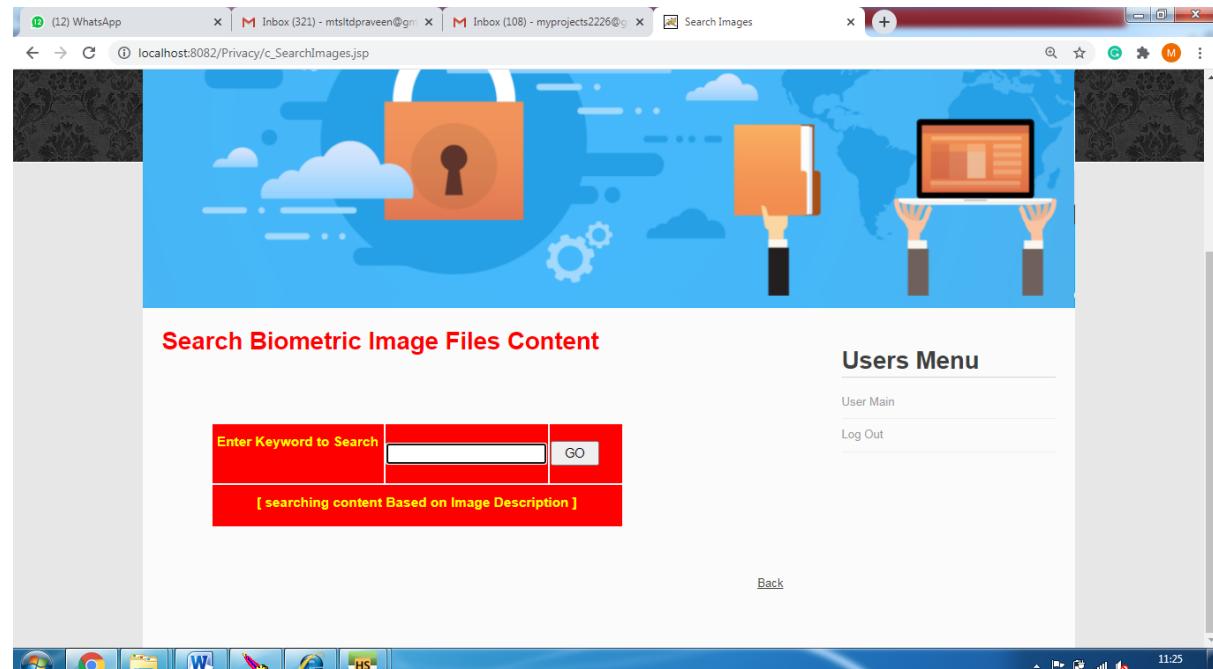


Comments..!

Commented By	Comments Details	Date
Amar	It is very useful	09/10/2018 12:57:43
tmksmanju	IT is useful in the crime activities	09/10/2018 16:14:26

[Back](#)

USER CAN DOWNLOAD THOSE IMAGES



Search Biometric Image Files Content

Enter Keyword to Search GO

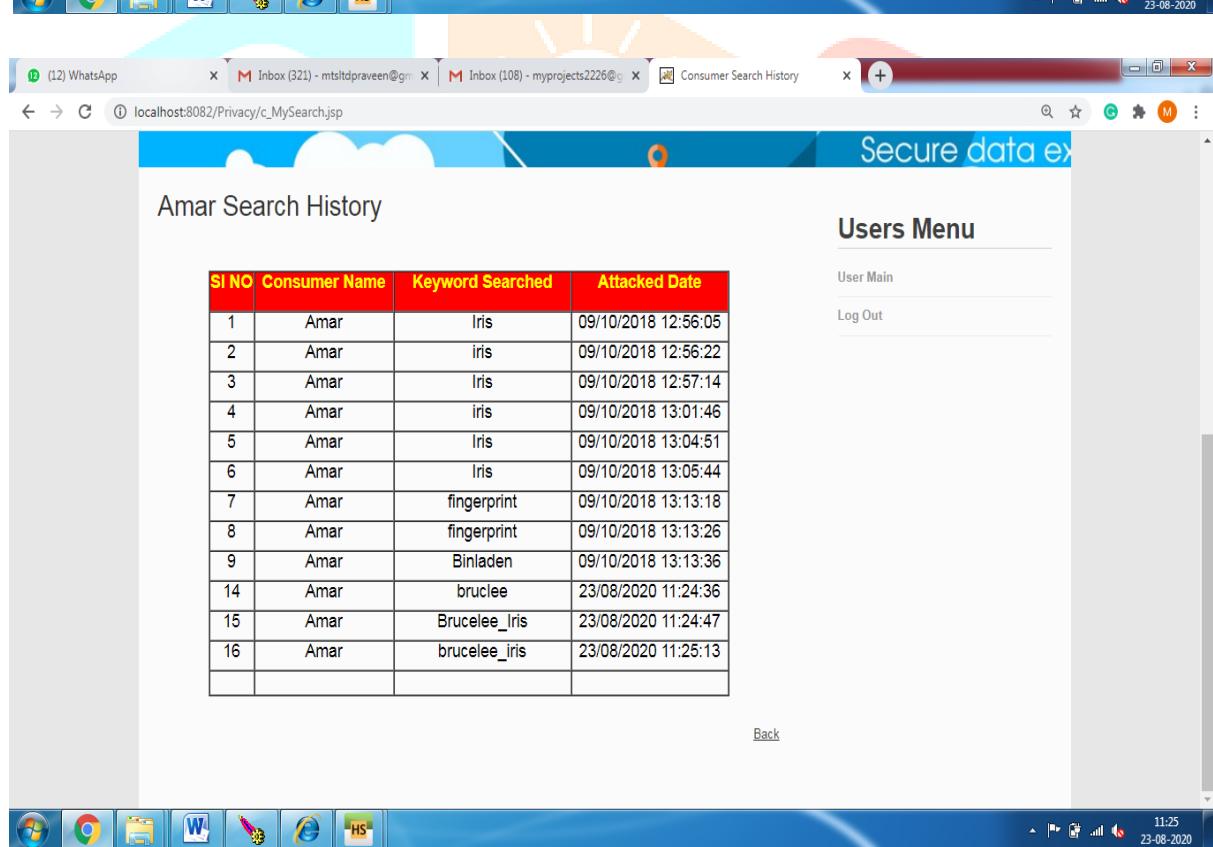
[searching content Based on image Description]

Users Menu

User Main

Log Out

Back



Secure data ex

Amar Search History

SI NO	Consumer Name	Keyword Searched	Attacked Date
1	Amar	Iris	09/10/2018 12:56:05
2	Amar	iris	09/10/2018 12:56:22
3	Amar	Iris	09/10/2018 12:57:14
4	Amar	iris	09/10/2018 13:01:46
5	Amar	Iris	09/10/2018 13:04:51
6	Amar	Iris	09/10/2018 13:05:44
7	Amar	fingerprint	09/10/2018 13:13:18
8	Amar	fingerprint	09/10/2018 13:13:26
9	Amar	Binladen	09/10/2018 13:13:36
14	Amar	brucelee	23/08/2020 11:24:36
15	Amar	Brucelee_Iris	23/08/2020 11:24:47
16	Amar	brucelee_iris	23/08/2020 11:25:13

Users Menu

User Main

Log Out

Back

7. CONCLUSION

This proposed work analyzed the mutual authentication scheme for cloud architecture proposed by Singhal *et al.* We have shown that their scheme is still vulnerable to various attacks. To overcome these security flaws, we have proposed a novel cloud authentication scheme using smartcard. The scheme achieves mutual authentication by using hash functions to protect user privacy. Performance comparison shows that the proposed scheme is efficient one.

8. REFERENCES

[1] D. Zisis 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 smartcard”, *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.