IMPROVING THE SECURITY AND EFFICIENCY OF CLOUD SERVICES THROUGH THE USE OF BIOMETRIC IDENTIFICATION

[1]Dr.S.V Sonekar,[2]Swati Raut,[3]Shubham Manuja,[4]Yash Telang
[1]Professor,[2]Assistant Professor,[34]Research Scholar
Department Of CSE
J D College of Engineering & Management, Nagpur

ABSTRACT_ Thus, there is an ever-increasing demand for secure remote access to remote data storage services in our data-driven culture." Here, we propose a new biometric authentication system for securing access to a distant server (in the cloud). We use biometric data as a secret credential in the suggested method. The user's biometric data is then utilised to construct the user's private key, which is unique to the individual. Using two biometric templates, we present an efficient method to generate a session key for secure message transmission between two participants. It's not necessary to store or share the user's private key in any way. Instead, the session key is produced automatically. In-depth testing and a side-by-by-side comparison show that the recommended strategy is effective and worthwhile.

1.INTRODUCTION

For example, according to the National Institute of Standards and Technologies (NIST), "Cloud Computing" is a model for making it possible to quickly provision, scale up or down, and release shared pools of configurable computing resources (networks and servers; storage; applications and services); this can be done with minimal management effort or provider interaction. Cloud has five primary traits that made it stand out from the rest. [1][3]: The ability to access cloud resources without the need for human intervention. Cloud resources can be accessed from a wide range of devices, including PCs, laptops, and mobile devices, across a wide range of networks. Virtual resources can be located in any location and assigned as needed, allowing for geographical independence. Rapid elasticity is a feature that allows users to swiftly increase or decrease the amount of resources they are using. Customers just pay for what they use in a measured service. With a variety of service models to choose from, the cloud is becoming a popular option for consumers that need a wide range of storage, processing power, productive apps and networking equipment in a variety of packages. (SaaS) programmes like Apple's MobileMe, Google Apps [5,] and Salesforce.com are examples of software as a service (SaaS) for consumers who just need to access the provider's applications. [6]. Google App Engine [7], force.com [8], and Microsoft Azure [8] are examples of PaaS providers that offer programming languages, libraries, services and tools enabling customers to build and deploy their own apps. The underlying cloud architecture is completely unmanageable for users of this service. To install their stuff on the cloud, users can utilise Amazon EC2 [9] and S3 [10], Sun Microsystems Cloud Services [11], and Dropbox [12], which all offer Infrastructure as a Service (IaaS) to give them access to basic cloud resources including operating systems, storage, and network components. End users have no idea where or how their data is stored or processed while using the cloud model. They only have access to it when it is made available to them. Authentication methods used to control and secure access to cloud data must be strong, as attackers target the methods that users employ to gain access to their data. One of the basic functions of authentication is the verification of specific information supplied by a user who has authentically logged into the system. An important part of cloud security is authentication. Knowledge-based authentication techniques, Possession-based authentication techniques, and Biometric-based authentication techniques are all examples of this type of authentication. [12][13]

2.LITERATURE SURVEY

By looking at a variety of authors' work, we can deduce the following facts about Biometric Two-Way Authentication:

Rajeswari is the name of the author. [1] In accordance with the new type of security mechanism established for the system, users were needed to provide multiple [two] biometric fingerprints in order to register. These templates are stored in the cloud by the service providers. Users can prove their identity using these fingerprint templates, which have to be supplied in the order of random integers. Fingerprint templates and images were sent even when encrypted. New model has three stages: registration, access and matching. Registration involves registering fingerprint images, which are then compared to a random number generator to generate a single-digit value for each of the two fingerprints. Access involves providing finger impressions, which are then compared to the random number generator's generated random number, and matching is where the two fingerprints are then verified. For the biometric photos, the elliptic curve algorithm and the Rivest–Shamir–Adleman (RSA) algorithm were utilised, respectively.

Author Hui Zhu [2] claims this. An online fingerprint authentication system called E-Finga encrypts outsourced data to safeguard user privacy. E-suggested Allows fingerprints to be outsourced to other servers with authorization from users so that service can be provided safely, precisely and efficiently without leaking of fingerprint information. An improved homomorphic encryption technology for secure Euclidean distance calculations over composite order groups is used in the proposed e-Finga to ensure the confidentiality of user fingerprints and the secrecy of matching templates.

Tian Yangguang comes in third. Using biometrics and homomorphic encryption, we hope to develop a mechanism for authenticating authorised remote users with an authentication server. Homomorphic encryption can be used to encrypt the identity information of authorised users in protocols such as TLS1.3 and QUIC. Homomorphic encryption primitives are used to verify the identity of the user. Full homomorphic encryption can easily handle all of the distance calculations above.

ShanmugaPriya, A Valarmathi, and D. Yuvaraj conducted this research. For cloud computing, this research suggests a new data security paradigm that is more secure than the current one. The suggested data security paradigm calls for OTP to be generated using HMAC for user authentication. This study also includes a comparison of MD5 and SHA algorithms in order to successfully execute the paradigm. The OTP method uses user-specific identifications such the International Mobile Equipment Identification (IMEI) and Subscriber Identification Module to construct an alphanumeric token with a limited lifespan (SIM). Two-way authentication is achieved by transmitting one-time passwords to the user's mobile device at the beginning of each login session. The use of a mobile phone as a verification instrument is required when using Dynamic one-time passwords with two-factor authentication.

He goes under the name Pietro Ruiu [5]. An authentication system for mobile devices based on Schnorr digital fingerprinting is presented in this study. UAC solutions can be found using keyboard dynamics, which is a common behavioural biometric. For example, keystroke dynamics are an example of behavioural biometrics that can be obtained without the user being aware of it being done. Voiceprint storage and transmission can now be made more secure with the use of homomorphic encryption, a technique that was developed by researchers. The OpenStack cloud platform is integrated with biometric authentication utilising fingerprints to build a complete Cloud system.

This group consists of six people: The Zhou Kai Jian Ren With our proposed threshold predicate (TPE) technique, the inner product of two vectors (x and y) can be compared to a predefined threshold using the TPE algorithm. Using TPE, it is impossible to learn anything about x or y other than the comparison result. Encrypted data can be processed using the suggested TPE in a compute-then-compare manner. Searching through encrypted data or using biometric identification are just two instances of how this computational model might be put to good use while still safeguarding individual privacy. Homomorphic encryption or two-party computing were employed to implement the systems. The templates and compare the distance with a predefined threshold should be able to establish how far apart they are from one another. The suggested TPE is compatible with both mobile phones and laptops.

This essay was written by Santosh Kumar [7]. We provide a biometric facial recognition technology to ensure the safety and privacy of cloud users while they utilise cloud resources. Here is a three-step procedure: extraction of facial features from pre-processed photos by photo-scanning (3) Finding out what makes a certain user special. When creating and decrypting biometric templates, paillier encryption and Eigen-face encoding algorithms are employed. The training and testing phases of the recognition system are separable. As the training process progresses, the recognition system builds a database of face images. The photos of the user's face are stored in the cloud-based biometric database. Biometric template database face features are compared to test (or query) photos in order to identify a person throughout a testing process, based on similarity scores.

Weixin [8] and Bian The fingerprint has long been considered a key biological feature in biometrics. It doesn't alter with time; it's personal to each person. PUFs have been used in authentication processes to prevent unauthorised access because of their distinctive physical feature. Bio-AKA, a new user authentication and key agreement method that fits all the criteria for high security, was built by utilising the inherent security qualities of fingerprint biometrics and PUFs. The suggested solution includes phases for user registration, login, and mutual authentication and key agreement.

Kumar Sarat[9] and Chand[10] For the first time, an authentication method as secure as passwords or keys is presented in this paper. When it comes to identifying people, biometrics refers to the utilisation of physiological traits. Each person's biometric data is unique to him or her. The biometric data of the user will be utilised in order to verify their identity. Using an encryption approach, both the user and the service provider's fingerprint images are protected. It's impossible for a hacker to decrypt a fingerprint image to get to the original image because of this. In Biometric Authentication, it is usual practise to employ two steps. Step one and step two are registering and identifying yourself.

Process. To use a biometric sensor, you must first input biometric data (such as a fingerprint) from the user. Features are extracted from the binary text using the feature extraction procedure (eliminates a redundancy). Service providers keep a user's feature vector in their database. Using this method, a user can log in to a cloud server from a faraway location. Received from feature extractor, matching module uses it to apply to feature vector extracted by extractor. The matching module intercepts the enrolling feature vector. The matching module runs an algorithm when a user tries to log in to see if their enrollment and identifying characteristics match..

3.PROPOSED SYSTEM

Here, we propose a new biometric authentication technique for granting safe access to a distant server (in the cloud). The biometric data of a user is treated as a secret credential in the suggested approach. Using the user's biometric data, we can then create a unique identity from which the private key can be generated. Using two biometric templates, we devise a fast method for generating a secure message transmission session key between two parties. It's not necessary to store or share the user's private key in any way. Instead, the session key is produced automatically.

3.1 IMPLEMENTATION

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

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

Users

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

Architecture Diagram

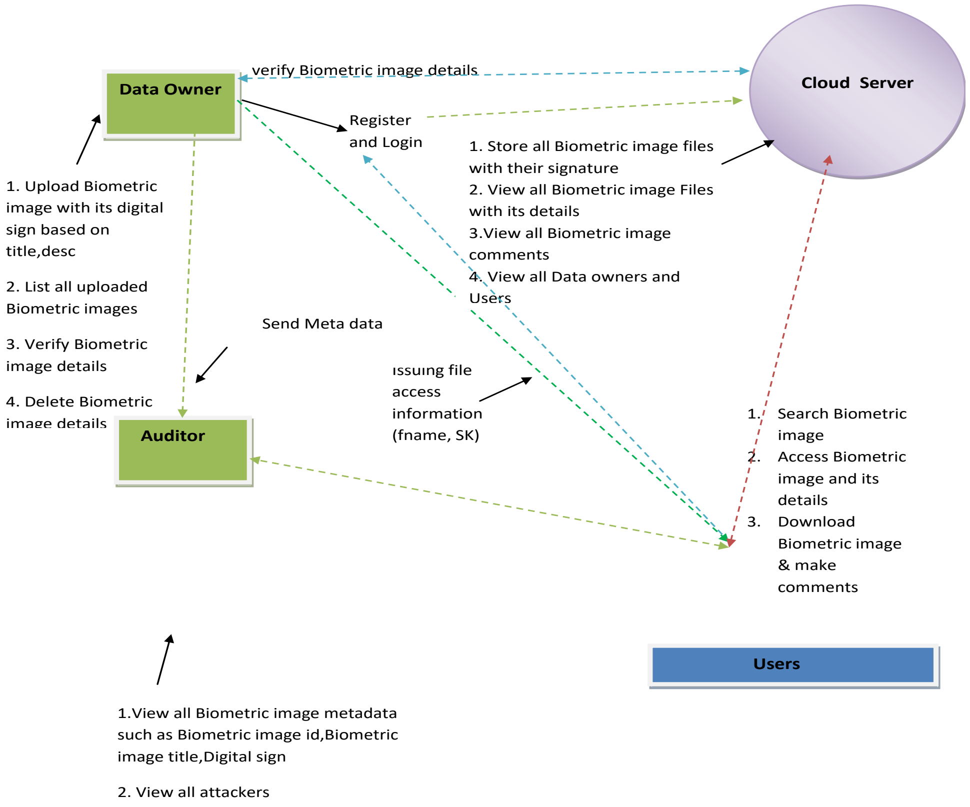
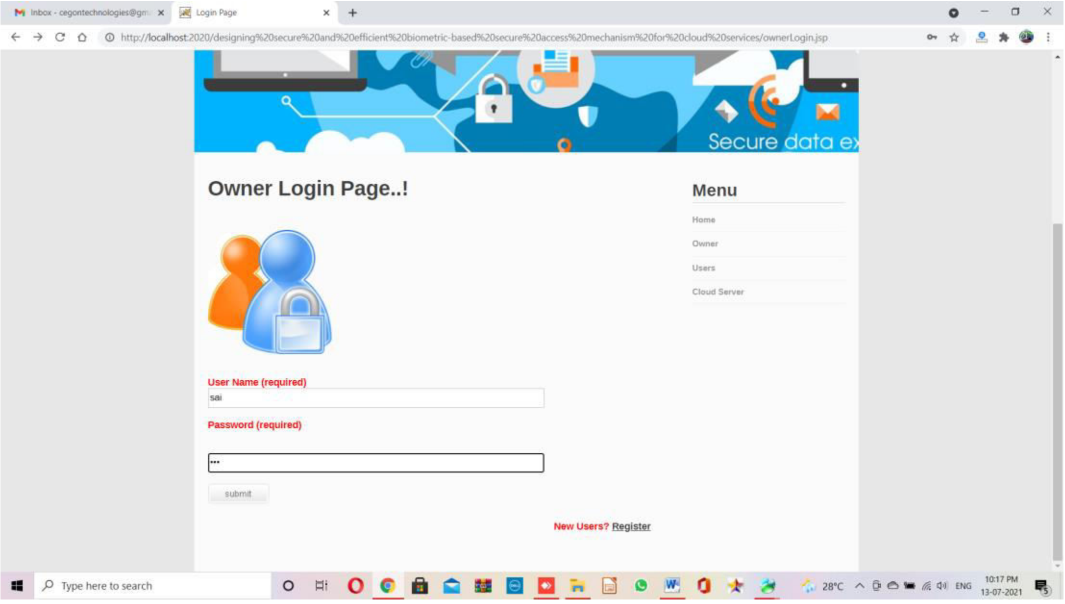

Data Owner
Cloud Server
verify Biometric image details
Register and Login
1. Store all Biometric image files with their signature
2. View all Biometric image Files with its details
3.View all Biometric image comments
4. View all Data owners and Users
1. Upload Biometric image with its digital sign based on title,desc
2. List all uploaded Biometric images
3. Verify Biometric image details
4. Delete Biometric image details
Send Meta data
ıssuıng file access information (fname, SK)
Auditor
1. Search Biometric image
2. Access Biometric image and its details
3. Download Biometric image & make comments
Users
1.View all Biometric image metadata such as Biometric image id,Biometric image title,Digital sign
2. View all attackers

Fig: 1. System Model

4.RESULTS AND DISCUSSION


Inbox - cegontechnologies@gm
Login Page
http://localhost:2020/designing%20secure%20and%20efficient%20biometric-based%20secure%20access%20mechanism%20for%20cloud%20services/ownerLogin.jsp
Secure data ex
Menu
Home
Owner
Users
Cloud Server
Type here to search
28°C
ENG
10:17 PM
13-07-2021

Owner Login Page..!

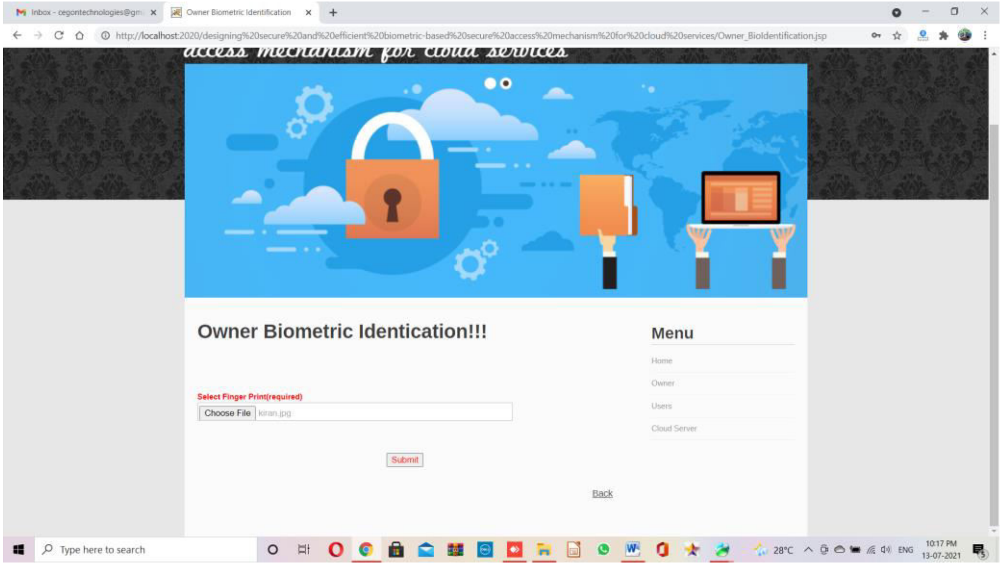
User Name (required)
sai

Password (required)
•••

submit

New Users? Register

Fig 4.1 Owner Login Form



http://localhost:2020/designing%20secure%20and%20efficient%20biometric-based%20secure%20access%20mechanism%20for%20cloud%20services/Owner_BioIdentification.jsp

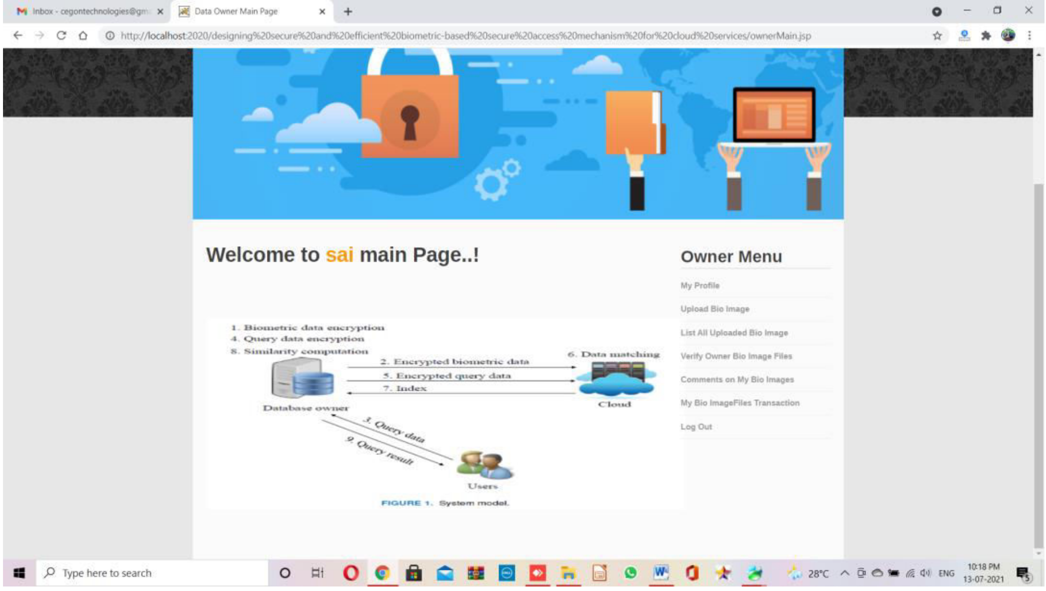
Owner Biometric Identication!!!

Select Finger Print(required)

Choose File kiran.jpg

Inbox - cegontechnologies@gm
Owner Biometric Identification
access mechanism for cloud services
Menu
Home
Owner
Users
Cloud Server
Submit
Back
Type here to search
28°C
ENG
10:17 PM
13-07-2021

Fog 4.2 in this page owner needs provide biometric image for login if the image is correct then owner can view his actions



http://localhost:2020/designing%20secure%20and%20efficient%20biometric-based%20secure%20access%20mechanism%20for%20cloud%20services/ownerMain.jsp

Welcome to sai main Page..!

FIGURE 1. System model.

Fig 4.3 owner main page

5.CONCLUSION

As indicated by the rising use of biometrics over more traditional security measures like passwords and tokens (e.g., on Android and iOS devices). Biometric-based authentication was presented in this study to allow remote users to access services and computing resources. As a result of our suggested method, it is able to construct private keys from fingerprint biometric reveals with 95.12 percent accuracy. There is no need to reveal any prior knowledge with our suggested session key creation method based on two biometric data. Several well-known attacks can be more robustly mitigated by the method we've taken as compared to other similar authentication protocols. Other biometric features and multi-modal biometrics for sensitive applications will be studied in the future (e.g., in national security matters).

REFERENCES

[1] A. Jain, L. Hong and S. Pankanti, “Biometric identification,” Communications of the ACM, vol. 43, no. 2, pp. 90-98, 2000.

[2] R. Allen, P. Sankar and S. Prabhakar, “Fingerprint identification technology,” Biometric Systems, pp. 22-61, 2005.

[3] J. de Mira, H. Neto, E. Neves, et al., “Biometric-oriented Iris Identification Based on Mathematical Morphology,” Journal of Signal Processing Systems, vol. 80, no. 2, pp. 181-195, 2015.

[4] S. Romdhani, V. Blanz and T. Vetter, “Face identification by fitting a 3d morphable model using linear shape and texture error functions,” in European Conference on Computer Vision, pp. 3-19, 2002.

[5] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, “A survey of key management schemes in wireless sensor networks,” Journal of Computer Communications, vol. 30, no. 11-12, pp. 2314-2341, 2007.

[6] X.Du,Y.Xiao,M.Guizani,andH.H.Chen,“Aneffectivekeymanagement scheme for heterogeneous sensor networks,” Ad Hoc Networks, vol. 5, no. 1, pp. 24-34, 2007.

[7] X. Du and H. H. Chen, “Security in wireless sensor networks,” IEEE Wireless Communications Magazine, vol. 15, no. 4, pp. 60-66, 2008.

[8] X.Hei,andX.Du,“Biometric-basedtwo-levelsecureaccesscontrolforimplantable medical devices during emergency,” in Proc. of IEEE INFOCOM 2011, pp. 346-350, 2011.

[9] X. Hei, X. Du, J. Wu, and F. Hu, “Defending resource depletion attacks on implantablemedicaldevices,”inProc.ofIEEEGLOBECOM2010,pp.1-5, 2010.

[10] M. Barni, T. Bianchi, D. Catalano, et al., "Privacy-preserving fingercode authentication," in Proceedings of the 12th ACM workshop on Multimedia and security, pp. 231-240, 2010.

[11] M. Osadchy, B. Pinkas, A. Jarrous, et al., "SCiFI-a system for secure face identification,"inSecurityandPrivacy(SP),2010IEEESymposiumon,pp. 239-254, 2010.