Review On Biometric Two-Way Authentication In Cloud Computing

Dolly Raja [1], Tosal Bhalodia[2], Rachana Buch[3]
Atmiya University, Rajkot.

ABSTRACT

The cloud computing is a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies and it has more advantage characters such as large scale computation and data storage, virtualization, high expansibility, high reliability and low price service. Over the last few years, cloud computing has become one of the fastest-growing IT environments for providing services to individuals and businesses of all sizes. Security is one of the critical challenges faced by cloud computing. Biometrics proves its efficiency to achieve secured authentication. We present a privacy-preserving online fingerprint authentication scheme. Single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system. So in this proposed system, we can provide Two-way authentication. In this, Two-way authentication we can provide better security against the single authentication because Two-way authentication adds a second level of authentication to an account login so, we can combine Fingerpr int Authentication and Password Authentication. It automated the verification method to match between two human fingerprints, where fingerprints are considered a commonly used biometrics to identify an individual and to verify their identity.

Keywords: Cloud Computing, Biometrics, Privacy, Security, Encryption, Decryption, Authentication.

I.INTRODUCTION

Cloud computing is the most promising and evolving network trend that provides opportunities to use infrastructure, application, or hardware as a service. Several organizations consider cloud computing to be secure, cost-effective, and suitable for their needs for sharing distributed resource services with the aid of Internet[1]. Large clouds, predominant today, often have functions distributed over multiple locations from central servers. If the connection to the user is relatively close, it may be designated an edge server.

Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing models. The availability of high-capacity networks, low-cost computers and storage devices as well as the wide spread adoption of hardware virtualization, service-oriented architecture and autonomic and utility computing has led to growth in cloud computing.

The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and helps the users focus on their core business instead of being impeded by IT obstacles.

There are many cloud computing characteristics are available such as On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured service. In the cloud computing various service models and deployment models are available. Service models are Software as a Service (SaaS), Platform as a Service (PaaS) and, Infrastructure as a Service (IaaS) . Deployment models are Private cloud, Community cloud, Public cloud, and Hybrid

cloud**.**

The main challenges for the cloud computing include the security, data privacy, and the personal data protection from the third party. Consequently, cloud computing is predominantly interesting with the biometric recognition to achieve scalability, accessibility, and availability[1].

Biometric-based identification which relies on personal biological or behavioral characteristics is receiving more and more attention as a convenient method of identifying people. Biometrics refers to an authentication scheme that measures automatically unique physical/human characteristics, such as fingerprint, voice, ear, eye color, iris, retina, and palmprint. **.** The major advantages of biometrics are (1) higher level of security of stored data (2) privacy preservation of users (3) diminutive chances of forgery and (4) cost-effective based solutions and (5) user friendliness[7].

One of the significant biometrics is the fingerprint as it is unique and consistent over the time. Thus, it can be used for identification and verification over a century. So In this paper for enhanced security we can provide the biometric two-way Authentication in cloud computing. In two-way authentication we can combine the fingerprint authentication and password authentication. Both authentication can be require to user login.

Two-phase are involved with this model:1) Registration Phase and, 2) Matching Phase. In this registration phase user can enroll with fingerprint and password and the matching phase it can match the enroll fingerprint with the user-provided fingerprint and it can also match the enroll password with the user-provided password. It is compulsory to match both of them to user login. If one of them is not match then user can not login successfully.

Since, encryption is the conversion of data into a form that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form. For enhanced security, the password from both user's and service provider's end can be encrypted. There are number of encryption algorithms that are used for the Password. One such algorithm is Advanced Encryption Standard that is adopted in this paper.

II. LITERATURE SURVEY

This section of Literature Survey eventually reveals some facts of Biometric Two-way Authentication based on the analysis of many authors work as follows:

Rajeswari, P.[1] The proposed system presented a new model of a security system, where the users were asked to provide multiple [two] biometric fingerprints during the registration for a service. These templates are stored at the cloud providers' end.The users are authenticated based on these fingerprint templates which have to be provided in the order of random numbers that are generated every time. Both fingerprint templates and images were provided whenever encrypted for enhanced security.Three phases are involved in the proposed new model, namely (i) the registration phase that enrolls with the two fingerprints, assigning single-digit values for each of two fingers; (ii) the access phase, where the finger impressions are provided in order of random number generated by a random number generator; and (iii) the matching phase that matches the user-provided fingerprints with the random numbers generated by a random number generator and encrypted image stored at the database. This new proposed model applied encryption algorithms for the two fingerprint inputs, namely the elliptic curve algorithm for the biometric images and the Rivest–Shamir–Adleman (RSA) algorithm for the numbers and mappings.

Zhu, Hui, [2] In this we present a novel privacy-preserving online fingerprint authentication scheme, named e-Finga, over encrypted outsourced data. In the proposed e-Finga scheme, the user's fingerprint registered in trust authority can be outsourced to different servers with user's authorization, and secure, accurate and efficient authentication service can be provided without the leakage of fingerprint information. Based on an improved homomorphic encryption technology for secure Euclidean distance calculation over composite order group, the proposed e-Finga can achieve the privacy of user fingerprint and confidentiality of matching templates.

Tian, Yangguang [3] In this work, we focus on biometric-based remote user authentication (BRUA) using homomorphic encryption, where authorized users wish to remotely authenticate to an authentication server using encrypted biometrics. Homomorphic encryption can be used to encrypt identity information of authorized users during the protocol execution and the protocols are TLS1.3 and QUIC. homomorphic encryption primitive is critical to the success of user authentication. Full homomorphic encryption can easily support all aforementioned distance calculations.

ShanmugaPriya, S., A. Valarmathi, and D. Yuvaraj [4]. This paper describes an enhanced approach for the already used data security model in cloud environment. The proposed data security model includes generation of OTP using HMAC for user authentication process. This paper also includes a comparative MD5 and SHA algorithms for the better implementation of the model. OTP algorithm powered with user's unique identifications like International Mobile Equipment Identification and Subscriber Identification Module makes a finite alphanumeric token valid for a session and for a single use. The cloud provides an initiated one time password scheme as a factor of two way authentication that sends a code to users mobile for every login session of the user. Therefore, for this scenario, we have proposed to make use of Dynamic one time password with two factor authentication as a Strong authentication technique, which requires mobile phone as an authentication device.

Ruiu, Pietro [5] In this paper, author involves a fingerprint biometric and password to enhance the security level of the remote authentication scheme for mobile device; paper proposes two-factor authentication scheme based on Schnorr digital signature and feature extraction from fingerprint. As a typical behavioral biometrics, some author use keystroke dynamics to obtain a UAC solution. The advantage of using behavioral biometrics such as keystroke dynamics is that it can be collected even without the knowledge of the user. Authors in improve the security of voiceprint storage and transmission, using an approach with homomorphic encryption. we present a complete Cloud system that uses biometric authentication based on fingerprints integrated with the OpenStack cloud platform.

Zhou, Kai, and Jian Ren [6] In this paper,our proposed threshold predicate encryption (TPE) scheme can encrypt two vectors x and y in such a manner that the inner product of x and y can be evaluated and compared to a pre-defined threshold. TPE guarantees that only the comparison result is revealed and no key information about x and y can be learned. The proposed TPE enables a compute-then-compare computational model over encrypted data. We show that such a computational model can be applied to many privacy preserving applications such as biometric identification and searching over encrypted data. The implementations were based on either homomorphic encryption and secure two-party computation. it should be able to determine the distance between the two templates and compare the distance with a threshold. the proposed TPE can be efficiently implemented on both mobile phones and personal laptops.

Kumar, Santosh [7] We propose a biometrics face recognition approach for security and privacy preservation of cloud users during their access to cloud resources.The proposed approach has three steps: (1) acquisition of face images (2) preprocessing and extraction of facial feature (3) recognition of individual using feature. Biometrics templates are generated and encrypted using paillier

Encryption algorithm and Eigen-face encoding algorithm. The recognition system consists of two phases: (1) training phase, and (2) testing phase. During the training phase of the system, the recognition system creates the database by the acquisition of individual face images. The face images are stored in the cloud biometric database. In the testing phase, it recognizes the individual based on the test(query) facial images by matching the similarity scores of facial features of the test images, stored in the biometric template database.

Bian, Weixin [8] The fingerprint has long been used as one of the most important biological features in the field of biometrics. It is person-specific and remain identical though out one's lifetime. Physically uncloneable functions (PUFs) have been used in authentication protocols due to the unique physical feature of it. In this paper, we take full advantage of the inherent security features of user's fingerprint biometrics and PUFs to design a new user authentication and key agreement scheme, namely Bio-AKA, which meets the desired security characteristics. The proposed scheme includes three phases: registration, login and the mutual authentication and key agreement phases.

Chand, K. Sarat, and B. Kezia Rani[9] In this paper, we are presenting a secure authentication mechanism unlike password or key which can't be hacked easily. Biometrics is an automatic identification of a person by using certain physiological features associated with the person. Biometrics data is unique for every individual. So our project aims at using Biometric data of user for the authentication process. The fingerprint images at both the user's end as well as the service provider's end are encrypted for providing better security using an encryption algorithm. Therefore, even if a hacker is able to gain access to a fingerprint image he will not be able to decrypt it to the original image. In general Biometric Authentication scheme consists of two stages: 1) Enrollment process , 2) Identification

Process. The user provides biometric information i.e. fingerprint to the biometric sensor, which converts the biometric data into a binary string. The feature extraction converts the binary string into a reduced representation set of features (eliminates a redundancy).The feature vector of a user is stored into a data base of service provider. In Identification when a user tries to log in into the remote cloud server, same steps will be executed. The feature vector is extracted by the feature extractor and submitted to matching module. The matching module intercepts the feature vector stored against user during enrolment process. The matching module executes the Algorithm to check the matching similarity between enrolment and identification feature process for the user trying to log in.

Hussein, Asmaa M., Hala M. Abbas, and Mostafa-Sami M. Mostafa [10] This study focuses on presenting a review on various biometric and non-biometric mechanisms for accessing cloud services. As declared before, techniques like passwords, smart card tokens, etc. have a certain basic drawback in ensuring the reality of the user who is accessing which is resolved with biometric techniques of human special characteristics. From comparing physiological biometrics to behavioral biometrics, we can figure that behavioral biometrics may not be so stable and accurate due to the changes of human behaviors. But, it provides a continuous and transparent authentication to the users, which overcome the issue of static authentication in physiological biometrics authentication. We will present a model of authentication using a combination of dynamic biometric with multi other factors for providing a system with high security rate.

Padma, P., and S. Srinivasan [11] The paper is an effort to perform a existing Biometric authentication techniques used to secure the data in cloud computing services. We have studied the physical traits based as well as the behavior traits based authentication techniques as a part of the biometric authentication. The entire authentication
Mechanism using bio-metric in Cloud can be broadly classified into 3 phases – the Registration phase, Log-in phase and the Verification phase. The registration phase is the initial phase wherein a user who prefers to use the Cloud service registers his biometric details with the cloud computing server. The login phase immediately succeeds the registration phase and is the phase wherein the biometric feature to facilitate access to Cloud is captured and verification for authentication is initiated. The actual authentication takes place in the verification phase.

Masala, Giovanni L., Pietro Ruiu, and Enrico Grosso [12] In this work is proposed a solution to ensure the data security and high availability of the resources, using an innovative distributed cloud storage architecture. The solution is based on data chunking technique: The basic idea is to share data in small chunks and spread them on different VMs

hosted on cloud computing.The system guarantees the identity of the users and makes easy, and secure, the access to data and services. Moreover, the adoption of a data chunking solution is proposed, which is based on a distributed cloud storage architecture. This provides protection of data residing also from provider's administrators and hardware supervisors. A further improvement of the system will extend biometric access to multimodal techniques, thus including face and face + fingerprint authentication.

III. CONCLUSION

Recently, biometrics based recognition systems have gained proliferation and more attention due to its inherent advantages. It efficiently provides the privacy preservation of cloud user and security of stored more sensitive data in the cloud servers . Thus, the recent research trend is emphasized towards addressing the issues of preservation of user's privacy, data integrity and management of growth of cloud data. Along with the privacy preservation of users, processing and maintain the data integrity, biometrics based recognition system retrieval has played an vital role to maintain the data in the cloud computing. As the biometric systems are playing a key role in government and commercial applications which are outsourced to the cloud, providing security and privacy of user is the biggest concern to be considered. Subsequently, the present work brings about a novel security model where fingerprints constitute an authentication.

The proposed system is an efficient technique of providing high-level security by combining fingerprint authentication and password authentication. It can be considered as a new security model of authentication, which provides high security from the intruders in the cloud. This novel and hybrid approach is theoretically portrayed to provide security for the biometric templates which enhances the privacy of the user.

REFERENCE

[1] Rajeswari, P., et al. "Multi-fingerprint unimodel-based biometric authentication supporting cloud computing." *Intelligent techniques in signal processing for multimedia security*. Springer, Cham, 2017. 469-485.

[2] Zhu, Hui, et al. "Efficient and Privacy preserving Online Fingerprint Authentication Scheme Over Outsourced Data." *IEEE Transactions on Cloud Computing* (2018).

[3] Tian, Yangguang, et al. "PriBioAuth: Privacy-Preserving Biometric-Based Remote User Authentication." *2018 IEEE Conference on Dependable and Secure Computing (DSC)*. IEEE, 2018.

[4] ShanmugaPriya, S., A. Valarmathi, and D. Yuvaraj. "The personal authentication service and security enhancement for optimal strong password." *Concurrency and Computation: Practice and Experience* (2019): e5009.

[5] Ruiu, Pietro, et al. "Accessing cloud services through biometrics authentication." *2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)*. IEEE, 2016.

[6] Zhou, Kai, and Jian Ren. "Passbio: Privacy-preserving user-centric biometric authentication." *IEEE Transactions on Information Forensics and Security* 13.12 (2018): 3050-3063.

[7] Kumar, Santosh, et al. "Privacy preserving security using biometrics in cloud computing." *Multimedia Tools and Applications* 77.9 (2018): 11017-11039.

[8] Bian, Weixin, et al. "Bio-AKA: An efficient fingerprint based two factor user authentication and key agreement scheme." *Future Generation Computer Systems* (2020).

[9] Chand, K. Sarat, and B. Kezia Rani."Biometric Authentication using SaaS in Cloud Computing." *International Research Journal of Engineering and Technology (IRJET)* 5.2 (2018).

[10] Hussein, Asmaa M., Hala M. Abbas, and Mostafa-Sami M. Mostafa. "Biometric-based Authentication

Techniques for Securing Cloud Computing Data-A Survey." *International Journal of Computer Applications* 975: 8887.

[11] Padma, P., and S. Srinivasan. "A survey on biometric based authentication in cloud computing." *2016 International Conference on Inventive Computation Technologies (ICICT)*. Vol. 1. IEEE, 2016.

[12] Masala, Giovanni L., Pietro Ruiu, and Enrico Grosso. "Biometric authentication and data security in cloud computing." *Computer and Network Security Essentials*. Springer, Cham, 2018. 337-353.

[13] Ilankumaran, S., and C. Deisy. "Multi-biometric authentication system using finger vein and iris in cloud computing." *Cluster Computing* 22.1 (2019): 103-117.

[14] Lu, Wei, et al. "Leveraging Cloud-Based Resources for Automated Biometric Identification." *Biometric-Based Physical and Cybersecurity Systems*. Springer, Cham, 2019. 437-454.

[15] Al-Assam, Hisham, Waleed Hassan, and Sherali Zeadally. "Automated biometric authentication with cloud computing." *Biometric-Based Physical and Cybersecurity Systems*. Springer, Cham, 2019. 455-475.

[16] Alsultan, Tarfah Mohammed, et al. "A Comparative Study of Biometric Authentication in Cloud Computing." *2019 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2019.

[17] Liu, Chun, et al. "An Efficient Biometric Identification in Cloud Computing With Enhanced Privacy Security." *IEEE Access* 7 (2019): 105363-105375.

[18] Gumaei, Abdu, et al. "Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation." *Journal of Parallel and Distributed Computing* 124 (2019): 27-40.

[19] Cheng, Hongbing, et al. "Identity based encryption and biometric authentication scheme for secure data access in cloud computing." *Chinese Journal of Electronics* 21.2 (2012): 254-259.

[20] Meena, Sunita, and Rupali Syal. "Authentication scheme in cloud computing: a review." *2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. IEEE, 2017.

[21] Pimple, Kshitij U., and Nilima M. Dongre. "Biometric Authentication in Cloud." *International Conference on Intelligent Data Communication Technologies and Internet of Things*. Springer, Cham, 2019.