SECURE AND EFFICIENT USER AUTHENTION SCHEME USING BIOMETRIC IN CLOUD SERVICE PLATFORM

Mr. P. Muthyalu , Assistant Professor, Dept of CSE, Narayana Engineering College Gudur
D. Sai Bindhu, Students, Dept of CSE, Narayana Engineering College Gudur
G. Pavithra, Students, Dept of CSE, Narayana Engineering College Gudur
G.Likitha, Students, Dept of CSE, Narayana Engineering College Gudur

Abstract – Rather than an on location server cloud services will be services that are accessible from a dispersed cloud stockpiling worker. These measured frameworks are worked by an outsider and give clients access to PC assets, for example, investigation or systems administration over the Internet. Cloud Computing is utilized to give processing assets over the Internet and is utilized to store information on cloud workers. Security and information insurance have been a critical field of interest in cloud processing because of the sharing of assets. Cloud service suppliers store and hold client data through server farms that are influenced by information spillage.. It is observed that many mechanisms have stressed data protection and have neglected privacy in the subsequent process. Authentication aids with preserving and verifying the identity of a recipient. That also suggests an effective technique to use two biometric models for safe message transmission to create a session key between two interacting parties. Finally, the reliability and utility of the proposed solution was seen by detailed trials and a comparative analysis.

Index terms – Authentication, biometric-based security, cloud service access, session key.

I. INTRODUCTION

Cloud services are a norm in our society. However, providing secure access to cloud services is not a trivial task, and designing robust authentication, authorization and accounting for access is an ongoing challenge, both operationally and research-wise[1][2]. A number of authentication mechanisms have been proposed in the literature, such as those based on Kerberos, OAuth and OpenID. Generally, these protocols seek to establish a secure delegated access mechanism among two communicating entities connected in a distributed system. These protocols are based on the underlying assumption that the remote server responsible for authentication is a trusted entity in the network[5][8]. Specifically, a user first registers with a remote server. This is needed to ensure the authorization of the owner. When a user wishes to access a server, the remote server authenticates the user and the user also authenticates the server. Once both verifications are successfully carried out, the user obtains access to the services from some remote server.

One key limitation in existing authentication mechanisms is that the user's credentials are stored in the authentication server, which can be stolen and (mis)used to gain unauthorized access to various services. Also, to ensure secure and fast communication, existing mechanisms generally use symmetric key cryptography, which requires a number of cryptographic keys to be shared during the authentication process. This strategy results in an overhead to the authentication protocols[3].

Designing secure and efficient authentication protocols is challenging, as evidenced by the weaknesses revealed in the published protocols. Therefore, in this paper it seeks to design a secure and efficient authentication protocol[4].

Specifically, first provide an alternative to conventional password-based authentication mechanism. Then, we demonstrate how one can build a secure communication between communicating parties involved in the authentication protocol, without having any secret pre-loaded (i.e., shared) information. In the proposed approach, we consider a fingerprint image of a user as a secret credential. From the fingerprint image, we generate a private key that is used to enroll the user's credential secretly in the database of an authentication server. In the authentication phase, we capture a new biometric fingerprint image of the user, and subsequently generate the private key and encrypt the biometric data as a query. This queried biometric data is then transmitted to the authentication server for matching with the stored data. Once the user is authenticated successfully, he/she is ready to access his/her service from the desired server. To obtain secure access to the service server, mutual authentication

between the user and authentication server, and also between the user and service server have been proposed using a short-term session key[6][7]. Using two fingerprint data, we present a fast and robust approach to generate the session key. In addition, a biometric based message authenticator is also generated for message authenticity purpose.

II. LITERATURE SURVEY

Based on the authentication types and factors being used, the user authentication protocols can be classified into three categories: 1) single-factor, 2) two-factor and 3) three-factor. In a single-factor authentication protocol, only one factor can be used (for example, user's smart card/mobile device or password or personal biometrics). In a two-factor authentication scheme, the user's smart card or mobile device and password can be used. On the other hand, in a three-factor authentication scheme, the user's smart card/mobile device, password and biometrics can be used.

Jiang et al. designed a password based user authentication scheme for wireless sensor networks (WSNs). This is a two-factor authentication scheme as it relies on both a smart card and some password. During the user registration process, an authorized user registers or re-registers with the trusted gateway node (GWN). The GWN then issues a smart card having the relevant credentials that are stored on the smart card. In addition, all the deployed sensor nodes are registered through a secure channel with the GWN and obtain their respective secret credentials. Using the pre-loaded credentials, a legitimate user authenticates with a designated sensor node with the help of the GWN during the login and authentication phases. However, Das later showed that this particular scheme is vulnerable to privileged insider attacks, where an internal user of the trusted authority (i.e., an insider attacker) having the registration information of a registered user can mount other attacks in the system, such as user impersonation attacks. Moreover, it was also shown that this scheme does not provide proper authentication, and fails to support new sensor node deployment in a target field. As a countermeasure, Das presented an improved and efficient three factor authentication scheme, where the three factors are a smart card, the user's password and the user's personal biometrics.

However, the scheme proposed by Das does not preserve sensor node anonymity. Althobaiti et al. proposed a biometric-based user authentication mechanism for WSNs. However, their scheme is insecure against impersonation attacks and man-in-the-middle attacks. Das then proposed a new biometric-based user authentication approach. Xue et al. also designed a temporal-credential-based mutual authenticated key agreement mechanism for WSNs. In their scheme, the remote authorized users are permitted to access authorized sensor nodes in order to obtain information and also to send some important commands to the sensor nodes in WSN. In this scheme, the GWN issues temporal credentials to each user and sensor node deployed in WSN with the help of the password-based authentication mechanism. Later, Li et al. demonstrated that Xue et al.'s scheme fails to resist stolen-verifier, offline password guessing, insider, many logged-in users, and smart card lost attacks. He et al. also demonstrated that Xue et al.'s scheme is insecure against user impersonation, off-line password guessing, modification and sensor node impersonation attacks.

Turkanovic and Holbl, and Turkanovic et al. proposed other user authenticated key agreement approaches. However, Turkanovic et al.'s scheme is insecure against smart card theft, offline password guessing, user impersonation, offline identity guessing, and sensor node impersonation attacks. Park et al. designed a privacy-preserving biometric-based user authentication mechanism using smart card, which uses hashing operation for biometric verification. However, the scheme is insecure against denial-of-service (DoS) attacks.

Dhillon and Kalra designed a biometric based user authenticated key agreement mechanism for secure access to services provided by Internet of Things (IoT) devices. Though this scheme uses lightweight operations, it does not protect against DoS attacks as it uses the perceptual hashing (biohashing) operation instead of fuzzy extractor. This is primarily because the biohashing technique hardly creates a unique value BH(BIOi) from the biometric data BIOi of a legitimate user Ui at different input times though it may reduce output error, where BH() is the biohashing function. Kaul and Awasthi designed an authenticated key agreement scheme, but it was later revealed to be insecure against user impersonation and off-line password guessing attacks.

In addition, the scheme of Kaul and Awasthi does not preserve user anonymity. Therefore, Kang et al. proposed an enhanced bioemtric-based user authentication scheme. However, this scheme is insecure against DoS attacks and also impersonation attacks where a privileged-insider attacker can easily mount such an attack.

Xia et al. designed a local descriptor, called the Weber local binary, to facilitate fingerprint liveness detection. Their mechanism is based on Support Vector Machine (SVM). In another work, Yuan et al. introduced a binary pattern (BP) neural network, which replies on fingerprint liveness detection. In their approach, the Laplacian operator is applied to obtain the image gradient values. After that, different parameters for the BP neural network are tested in order to attain superior detection precision. It refers the interested reader for a comprehensive literature review of fingerprint-based biometric authentication methods.

Huang et al. introduced two different specific security threats based on the smart-card-based password authentication mechanisms for distributed system. In their system, a user needs valid smart card and corresponding password to have a successful authentication. They also considered two different adversaries: first one is an adversary having pre-computed data stored in smart card and second one is an adversary having with different data stored in smart card.

Wang and Wang introduced different property of user privacy perversion in two-factor authentication schemes for wireless sensor networks (WSNs). They designed two different representative schemes to reveal the challenges and subtleties in designing two-facto authentication for privacy preserving for WSNs. They also introduced a game-based security model for two-factor authentication.

Wang et al. proposed three different identity-based user authentication schemes to reveal the challenges in authentication schemes for mobile devices. They also considered sessionspecific temporary information attack, impersonation attack and also poor usability. Several other authentication protocols have been also proposed in the literature to provide the security in wireless sensor networks and mass storage devices.

III. PROPOSED SYSTEM

In the proposed approach, let consider a fingerprint picture of a client as a mystery qualification. From the fingerprint picture, then create a private key that is utilized to enlist the client's certification covertly in the database of an authentication server. In the authentication stage, we catch another biometric fingerprint picture of the client, and hence produce the private key and scramble the biometric data as a question. This questioned biometric data is then communicated to the authentication server for coordinating with the put away data. When the client is validated effectively, he/she is prepared to access his/her service from the ideal server. To get secure access to the service server, common authentication between the client and authentication server, and furthermore between the client and service server have been proposed utilizing a transient session key.

Utilizing two fingerprint data, we present a quick and powerful way to deal with create the session key[1]. Likewise, a biometric-based message authenticator is produced for message realness purposes.

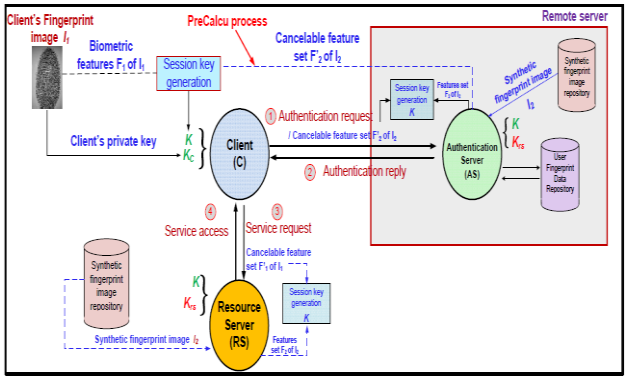

Fig. 1: System model

Proposal framework

In this segment, initially talk about the system model and threat model utilized in the proposed biometric-based authentication protocol (BioCAP), prior to introducing the different stages in BioCAP.

A. System Model An outline of BioCAP is appeared in Fig. 1, which involves three elements. These elements are the client(s) (C), authentication server(s) (AS), and some asset server (RS). AS contains a database of clients' enlisted data, while AS creates RS's private key during the sending stage and it is divided among AS and RS. Likewise, both AS and RS incorporate an enormous vault of a comparative arrangement of engineered fingerprint pictures. Some manufactured fingerprint databases, for example, some openly accessible databases, are utilized in the proposed approach. At the point when C wishes to access a service from RS, C initially sends an authentication solicitation to AS. AS checks C's solicitation and sends an answer message to C upon fruitful confirmation. When C acquires the authentication answer message, C sends a service solicitation to RS for getting access. RS at that point confirms the service demand. On the off chance that the service demand is confirmed effectively, RS sends an answer to C. C and RS commonly validate one another. A session key among C and AS, and C and RS are utilized for resulting secure message interchanges. Further, the message legitimacy is constrained by a message authenticator. BioCAP has two key cycles, to be specific: client enrollment and client authentication. The client enlistment requires a private key generation, though client authentication requires the generation of the session key and the message authenticator. BioCAP gives an arrangement to turn over the private key of a client. Additionally, BioCAP is secure, computationally more affordable, and defeats the inborn shortcomings of biometric confirmation. Also, BioCAP doesn't require pre-shared keys, and gives a smooth common authentication system, and requests less number of keys to be overseen from application and client perspective.

Threat Model

Follow the comprehensively acknowledged "Dolev-Yao (DY) threat model" [10] in this paper. The DY model allows a foe, state A not exclusively to block the messages during correspondence yet in addition permits to alter, erase, or even infuse bogus messages during correspondence among the organization substances. Along these lines, under the DY model, the correspondence among the organization elements occurs over a public channel. We further accept that the customers are not confided in the organization, though the authentication servers (AS) and asset server (RS) are semiconfided in substances in the organization. In a secret phrase based authentication component, a secret word speculating assault is practical if low-entropy passwords are utilized.

Then again, in a biometric-based authentication instrument, biometric data speculating assault utilizing savage power assaults is computationally infeasible. Be that as it may, A can perform other likely assaults, for example, replay, manin-the-center, advantaged insider, refusal of-service and biometric data speculating assaults, and furthermore taken savvy card and secret word speculating assaults (for secret word based authentication plans). Likewise, A can alter put away biometric data and with taken biometric data.

Client's Private Key Generation From a caught client's fingerprint picture, we extricate all details focuses. To expand the exactness in element extraction, we initially adjust the fingerprint picture. From this adjusted fingerprint picture, we select the predictable district. The reliable area can be characterized as the fingerprint locale, which has a high possibility of showing up in any caught fingerprint picture. We select this predictable area to separate the particulars focuses. To choose a bunch of details focuses from the predictable district, we propose to utilize a level section. The even section is a little territory of the steady locale, which has the most noteworthy number of particulars focuses.

Session Key Generation

To produce a session key between two standards P1 (state, customer C) and P2 (state, authentication server AS), we take two diverse biometric fingerprint data. P1 takes C's fingerprint picture and P2 takes a manufactured fingerprint picture. The session key generation measure is indicated as the PreCalcu cycle. This cycle begins execution when P1 loads its application to start a session.

PreCalcu Step-1 and PreCalcu Step-2 – see Fig. 2. At the point when an application is stacked in P1's machine, P2's will run PreCalcu Step-1. At the point when P1 gets an answer from P2, P1 runs PreCalcu Step-2.PreCalcu Step-1: In this cycle, P2 haphazardly chooses a manufactured fingerprint picture from the engineered fingerprint database. Let Sth manufactured fingerprint picture (say I2) be arbitrarily chosen by P2, where $1 \leq S \leq Sh$, Sh is the complete number of engineered fingerprint pictures in the database.

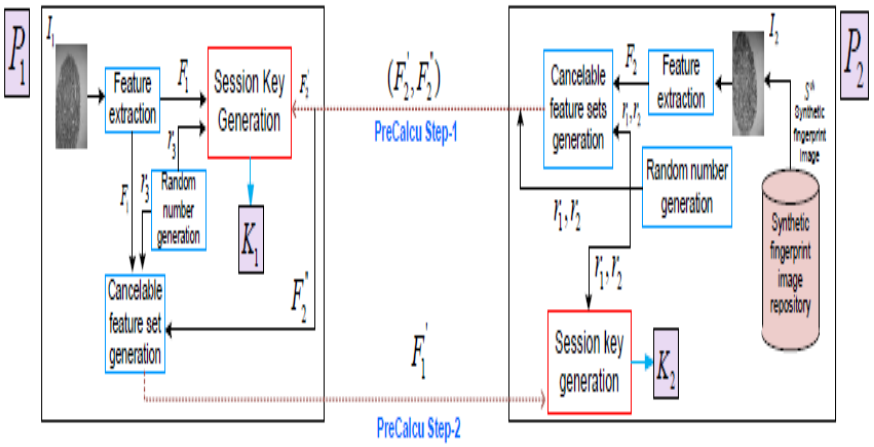

Fig.2: *PreCalcu* Process

User Authentication

A user's authentication cycle starts with the session key generation with the PreCalcu cycle. Let, the session key among C and as of now be K. The user authentication measure is done in two stages. In the primary stage, C brings the mystery Kr0 from the database of AS. In the subsequent stage, C uses the got mystery (Kr0) to send his biometric highlight to AS for confirmation purpose.

IV. CONCLUSION

Biometric has its extraordinary favorable circumstances over regular secret word and token-based security system, as confirmed by its expanded appropriation (e.g., on Android and iOS gadgets). In this paper, we acquainted a biometric-based component with validate a user trying to access services and computational assets from a distant area. Our proposed approach permits one to create a private key from a fingerprint biometric uncovers, as it is conceivable to produce a similar key from a fingerprint of a user with 96.72% exactness. Our proposed session key generation approach utilizing two biometric data doesn't need any earlier data to be shared. An examination of our methodology with other comparative authentication protocols uncovers that our protocol is stronger to a few known assaults.

REFERENCES

1. C. Neuman, S. Hartman, K. Raeburn, “The kerberos network authentication service (v5),” RFC 4120, 2005.
2. “OAuth Protocol.” [Online]. Available: http://www.oauth.net/
3. “OpenID Protocol.” [Online]. Available: http://openid.net/
4. G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kerberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.
5. Ravinder Rao, P., Sucharita, V.A framework to automate cloud based service attacks detection and prevention. International Journal of Advanced Computer Science and Applications, 2019, 10(2), pp. 241–250
6. Kehne, J. Schonwalder, and H. Langendorfer, “A nonce-based protocol for multiple authentications,” ACM SIGOPS Operating System Review, vol. 26, no. 4, pp. 84–89, 1992.
7. B. Neuman and S. Stubblebine, “A note on the use of timestamps as nonces,” Oper. Syst. Rev., vol. 27, no. 2, pp. 10–14, 1993.
8. Penchalaiah P, Rajasekar P, Srinivas Viswanth V and Ramesh Reddy (2020), “An Efficient Multi-User Hierarchical Authenticated Encryption Using Simultaneous Congruence For Highly Secure Data”, International Journal of Future Generation Communication And Networking, ISSN/eISSN 2233-7857/2207-9645, 30 Jun 2020, vol. 13, no.2 , pp. 1-10, 10.33832/ijfgcn.2020.13.2.01
9. J. Astorga, E. Jacob, M. Huarte, and M. Higuero, “Ladon : endto- end authorisation support for resource-deprived environments,” IET Infomration Security, vol. 6, no. 2, pp. 93–101, 2012.
10. Rao, P.R., Sucharita, V.A secure cloud service deployment framework for DevOps Indonesian Journal of Electrical Engineering and Computer Science, 2020, 21(2), pp. 874–885
11. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, “SPINS: security protocols for sensor networks,” ACM Wireless Networking, vol. 8, no. 5, pp. 521–534, 2002.
12. P. Kaijser, T. Parker, and D. Pinkas, “SESAME: The solution to security for open distributed systems,” Computer Communications, vol. 17, no. 7, pp. 501–518, 1994.