DESIGNING SECURE AND EFFICIENT BIOMETRIC-BASED SECURE ACCESS MECHANISM FOR CLOUD SERVICES

P.Vijay Bhaskar Reddy, Associate Professor, Dept.of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP

T.Ajay Kumar, PG Scholar, Department of Master of Computer Applications Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP

Abstract

The demand for remote data storage and computation services are increasing exponentially in our data-driven society; thus, the need for secure access to such data and services. In this paper, we design a new biometric-based authentication protocol to provide secure access to a remote (cloud) server. In the proposed approach, we consider biometric data of a user as a secret credential. We then derive a unique identity from the user's biometric data, which is further used to generate the user's private key. In addition, we propose an efficient approach to generate a session key between two communicating parties using two biometric templates for a secure message transmission. In other words, there is no need to store the user's private key anywhere and the session key is generated without sharing any prior information. A detailed Real-Or- Random (ROR) model based formal security analysis; informal (non-mathematical) security analysis and also formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool reveal that the proposed approach can resist several known attacks against (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utility of the proposed approach.

Keywords: Authentication, biometric-based security, cloud service access, session key.

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. 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. 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. Designing secure and efficient authentication protocols is challenging, as evidenced by the weaknesses revealed in the published protocols of Jiang et al. Althobaiti et al. ,Xue et al.,Turkanovic et al. Park et al. Dhillon and Kalra Kaul and Awasthi and Kang et al.Therefore, in this paper we seek to design a secure and efficient authentication protocol. Specifically, we will 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.

Statement of the Problem

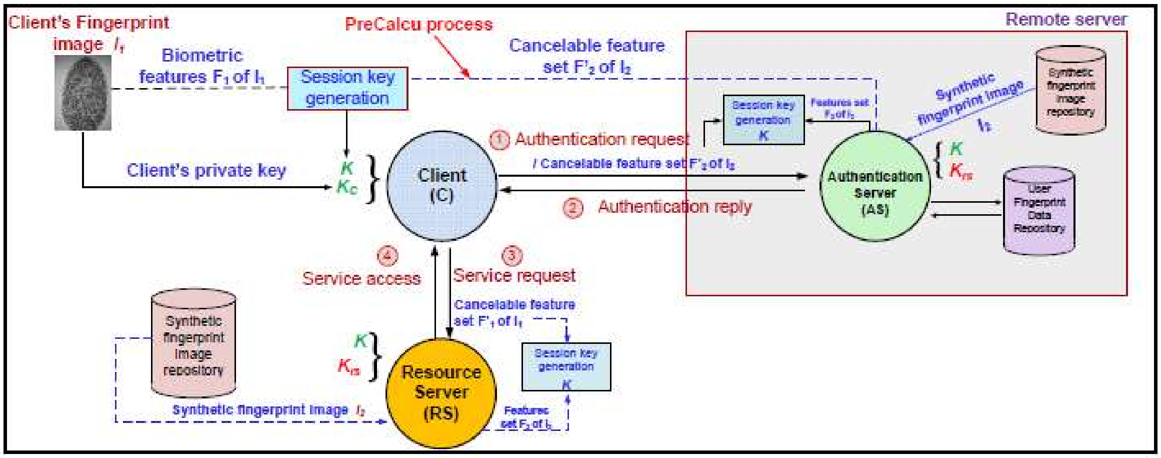
In existing authentication mechanisms is that the user's credentials are stored in the authentication server, which can be stolen, and (mis)used to gain unauthorized access to various services.Also, to ensure secure and fast communication, existing mechanisms generally use symmetric key cryptography,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

Objectives of the study

- An effective way to transmit the user's biometric data through the unsecured network channels to an authentication
- We propose an approach to generate a revocable private key directly from an irrevocable fingerprint image. There is no need to store the private key or a direct form of the user's biometric data anywhere.
- We mitigate the limitation in traditional mechanisms that require the user's credentials to be stored in the authentication server.
- We introduce a novel way to generate session keys.
- In traditional authentication protocol, each entity requires some preloaded information; thus, incurring some overhead. We introduce a new mechanism to avoid the need for secret pre-loaded information.
- A message authentication mechanism, as an alternative to the existing message authentication protocols (i.e., Message Authentication Code (MAC)), is introduced.

Review of Literature

In this section, we mainly discuss existing biometric-based user authentication schemes that have been presented in the literature. 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.


Client's Fingerprint image I_1
PreCalcu process
Biometric features F_1 of I_1
Session key generation
Cancelable feature set F'_2 of I_2
Remote server
Session key generation K
Features set F_2 of I_2
Synthetic fingerprint image I_2
Synthetic fingerprint image repository
① Authentication request
/ Cancelable feature set F'_2 of I_2
Client's private key
K
K_c
Client (C)
Authentication Server (AS)
K
K_{rs}
User Fingerprint Data Repository
② Authentication reply
④ Service access
③ Service request
Cancelable feature set F'_1 of I_1
Synthetic fingerprint image repository
K
K_{rs}
Resource Server (RS)
Session key generation K
Synthetic fingerprint image I_2
Features set F_2 of I_2

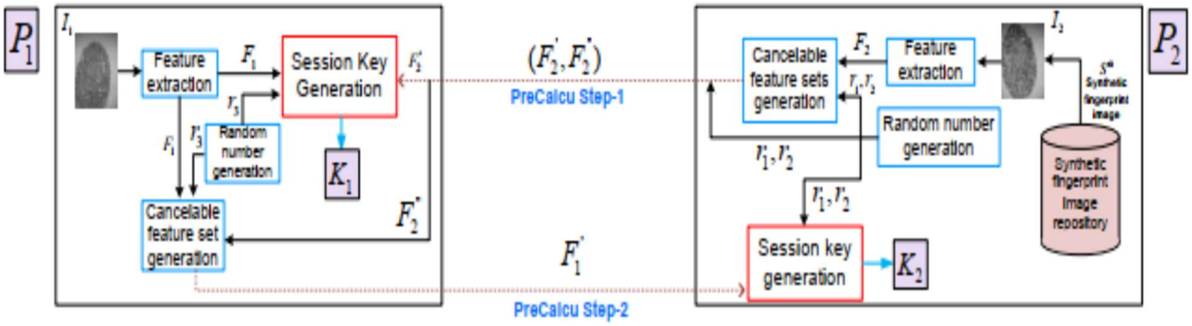
Research Methodology

In the proposed approach, we consider a fingerprint picture of a client as a mystery qualification. From the fingerprint picture, we 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. Likewise, a biometric-based message authenticator is produced for message realness purposes.

PROPOSAL FRAMEWORK: In this segment, we 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. 3, 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: We follow the comprehensively acknowledged "Dolev-Yao (DY) threat model" 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 semi confided 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.

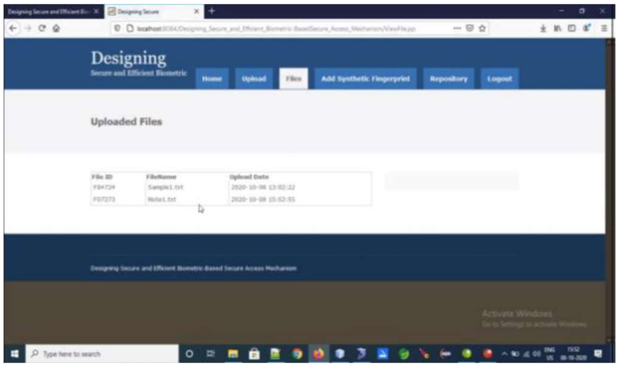
SESSION KEY GENERATION: To produce a session key between two standards P1 (state, customer C) and P2 (state, authentication server AS), we take two diverse biometric fingerprint data. P1 takes C's fingerprint picture and P2 takes a manufactured fingerprint picture. The session key generation measure 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. 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 ≤ S ≤ Sh, Sh is the complete number of engineered fingerprint pictures in the database.

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.

Results and Discussion

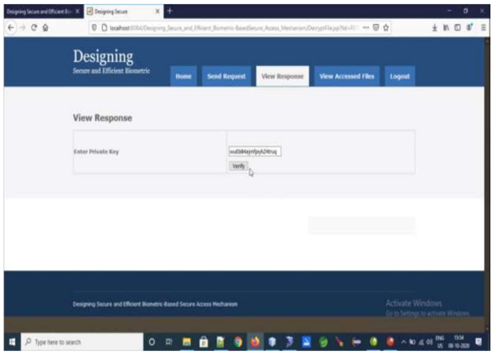

Designing Secure and Efficient Bi...
Designing Secure
localhost:8084/Designing_Secure_and_Efficient_Biometric-BasedSecure_Access_Mechanism/ViewFile.jsp
Designing
Secure and Efficient Biometric
Home
Upload
Files
Add Synthetic Fingerprint
Repository
Logout
Type here to search

Uploaded Files

File ID	FileName	Upload Date
F84724	Sample1.txt	2020-10-08 13:02:22
F07273	Nota1.txt	2020-10-08 15:52:55

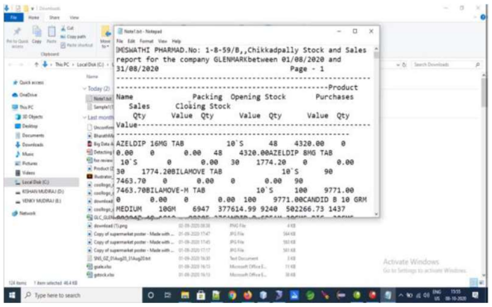
Designing Secure and Efficient Biometric-Based Secure Access Mechanism

Resource Server


Designing
Secure and Efficient Biometric
Home
Send Request
View Response
View Accessed Files
Logout
Verify
Designing Secure and Efficient Biometric-Based Secure Access Mechanism
Activate Windows
Go to Settings to activate Windows.
Type here to search

View Response

Enter Private Key: xud3d4ajmfpyh24truq



```
MESWATHI PHARMAD.No: 1-8-59/B,,Chikkadpally Stock and Sales
report for the company GLENMARKbetween 01/08/2020 and
31/08/2020                                   Page - 1
-------------------------------------------------------------
-----------------------------------------------------Product
Name                 Packing  Opening Stock        Purchases
   Sales       Closing Stock
    Qty        Value  Qty        Value  Qty        Value  Qty
Value--------------------------------------------------------
------------------------------------------------------
AZELDIP 16MG TAB           10`S      48    4320.00    0
0.00    0       0.00   48    4320.00AZELDIP 8MG TAB
 10`S      0       0.00   30    1774.20    0       0.00
30    1774.20BILAMOVE TAB               10`S      90
7463.70    0       0.00    0       0.00   90
7463.70BILAMOVE-M TAB            10`S      100    9771.00
0       0.00    0       0.00  100    9771.00CANDID B 10 GRM
MEDIUM    10GM    6947  377614.99 9240  502266.73 1437
```

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] Panchal, G., Samanta, D., Das, A. K., Kumar, N., & Choo, K. K. R. (2020). Designing Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services. IEEE Transactions on Cloud Computing.

[2] Batool, R., Naveed, G., & Khan, A. (2015). Biometric authentication in cloud computing. Int J Comput Appl, 129(11), 6-9.

[3] Identity, C. B. (2016). Authentication: BIOMETRICS-AS-ASERVICE.

[4] https://books.google.com/books?id=RYlJDQAAQBAJ

[5] Gawande, Ujwalla & Golhar, Yogesh & Hajari, Kamal. (2017). Biometric-Based Security System: Issues and Challenges. 10.1007/978-3-319-44790-2_8.

[6] Kohl, J., & Neuman, C. (1993). The Kerberos network authentication service (V5). RFC 1510, September.

[7] IDFusion: An open architecture for Kerberos based authorization.

[8] Kehne, A., Schönwälder, J., & Langendörfer, H. (1992). A nonce based protocol for multiple authentications. ACM SIGOPS Operating Systems Review, 26(4), 84-89.

[9] Neuman, B. C., & Stubblebine, S. G. (1993). A note on the use of timestamps as nonces. ACM SIGOPS Operating Systems Review, 27(2), 10-14.

[10] D. Dolev and A. C. Yao, "On the security of public-key protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198– 208, 1983.

[11] K GURNADHA GUPTA"Implementation of dynamic cloudlet system for energy optimization in cloud computing" proceedings of 7th International CONFERENCE ON INNOVATIONS IN COMPUTER SCIENCE & ENGINEERING, ICICSE-2019, GURUNANAK INSTITUTIONS, HYDERABAD Volume 1 Issue 1 Page 105-109.

[12] Kurikala, G., Gupta, K. G., & Swapna, A. (2017). Fog computing: Implementation of security and privacy to a comprehensive approach for avoiding knowledge thieving attack exploitation decoy technology.International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2(International Journal of Engineering Research & Technology (IJERT).

[13] Penchalaiah, P., & Rajasekar, P. An Efficient Multi-User Hierarchical Authenticated Encryption Using Simultaneous Congruence for Highly Secure Data. International Journal of Future Generation Communication and Networking (WoS), ISSN, 2233-7857.