International Conference on Advances in Materials, Computing and Communication Technologies
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

A Secure Remote Biometric Based Finger Print for Distributed Mobile Cloud Computing Environment

A. Abisha[1], Mrs. C. Felsy[2], Mrs. M. L. Sworna Kokila[3], Mrs. M. Manchu[3]
[1]PG Scholar, Ponjesly College of Engineering, Nagercoil, Tamil Nadu, India
[2]Assistant Professor, Ponjesly College of Engineering, Nagercoil, Tamil Nadu, India
[3]Associate Professor, Ponjesly College of Engineering, Nagercoil, Tamil Nadu, India

ABSTRACT

Identity based Mutual Authentication and Key Agreement (ID-MAKA) between a versatile client and cloud benefit supplier is vital for getting to any cloud administrations. In later a long time, there are a huge number of ID-MAKA plans had been proposed on versatile cloud computing administrations to form confirmation and getting to prepare more ease of use, security, and adaptability. To a modern ID-MAKA plot for versatile cloud computing, which firstly accomplishes farther biometric based verification (inaccessible servers confirm user's biometrics), single sign-on (a single credential and single enrollment for getting to numerous servers) and center-less verification (the registration center does not take part within the get to method) in one plot. In arrange to realize this target, to plan a ZK token based on ECC and cryptographic hash work, and after that shrewdly utilize it to present the fuzzy extractor innovation and zero-knowledge innovation into our plot. Hence, the client can get to different cloud computing servers by enrolling as it were once within the enrollment center, and cloud computing servers can total the biometric-based inaccessible verification and key assention for the client without the enrollment center taking part. In this way, the conspire significantly makes strides ease of use, adaptability, and security compared to other existing arrangements. To provide a formal security verification for our plot by utilizing Real-Or-Random (RoR) demonstrate and Burrows Abadi Needham (Boycott) rationale to appear that the display conspire is secure and security investigation for other known assaults. At long last, agreeing to the explore result, the plot has lower computation and communication fetched compared with most existing related plans.

I. INTRODUCTION

Mobile computing depends on the ability to use computer resources through mobile devices. Moreover, mobile computing enables the execution of tasks that have been traditionally done by normal desktops. In general, mobile computing is supported by three basic concepts: hardware, software, and communication. Hardware constitutes devices that can be utilized by users. Software includes applications designed and developed to execute tasks in a mobile environment and communication which includes networks and protocols that can support the communication aspects of mobile computers such as Wireless Local Area Networks (WLAN), Long-Term Evolution 4G LTE and satellite networks. The mobile computing environment supports the following. First, there is mobility which allows mobile nodes or fixed nodes to connect with other devices' nodes in the mobile computing environment through Mobile Support Station (MSS). Second, diversity of network access types refers to mobile nodes which can communicate using various types of access networks. Third, frequent network disconnection means mobile nodes are not able to keep the connection consistent because of limited mobile nodes' resources such as battery energy and communication bandwidth. Fourth, regarding the issue of poor reliability and security, mobile node signals suffer from interference in mobile networks which make security increasingly more important in mobile computing.

Biometrics based authentication using cryptographic hash functions, and formally defined security requirements for biometrics-based authentication including confidentiality, integrity and availability. Notice that some research work in the literature assume that the biometrics is a public value (such as fingerprint and face), and their privacy concern is the relationship between a biometric information and user's real identity. However, three- factor and multi-factor authentication (such as smart card, password and biometrics) in the literature formed an opposite research direction, such that biometrics acts as a secret key for (remote) user authentication, and the proposed three/multi-factor solutions are able to provide enhanced security on user authentication. Meanwhile, another research line also confirmed this assumption. One well-known threefactor authentication was done by Fan and Lin in which an efficient three- factor authentication with privacy protection on biometrics was proposed, and formally proven in Bellare and Rogaway's model. Specifically, they require user's biometrics is not sharing with remote server, and the biometrics matching is performed by remote server.

Moreover, some research work focused on privacy-preserving (remote) user biometrics authentication/identification, and a few novel solutions are mainly for biometrics identification in the cloud. For instance, proposed to use a homomorphic encryption scheme for efficient biometric authentication by employing multi-party computation techniques. Wang et al. used invertible matrices as symmetric-key secrets to encrypt biometrics and the exact biometrics matching are executed in the transformed (i.e., encrypted) domain, namely, transformation based cancellable biometrics. To compare our proposed solution with typical works on biometric-based authentication/identification to highlights our distinctions: it shows that our proposed solution is the first lightweight biometrics based remote user authentication with leakageresilient and biometrics privacy.

"Fast Identity Online" (FIDO) alliance is an industry consortium to address the lack of interoperability between authentication devices and user authentication experiences. Specifically, FIDO is used to enhance user authentication security (e.g., 5 using biometrics) on local devices, while we focus on remote biometric-based user authentication in this work.

A. Existing System

In existing work, a Registration Server (RS) delivers a link to all the users who have performed registration successfully, and then each user uses the link to obtain and install software in their device while also providing their credentials (password, identity and biometric signature.) Note that while the password may be guessed, it is hard to guess biometric signatures.

Then, the software encrypts important files by using a negotiated key to provide security on the storage file. Whenever, the user of that device wants to access that file, RS first verifies the user and then provides a decryption key to recover the original file. All the files are then encrypted using a new session key. However, we argue that a storage device will still not be completely security protected. Hence, we have devised a standard security protocol which protects the storage device to defend unauthorized access. Firstly we have used the concept of biometric data along with a password in our protocol, hence it is difficult to guess the password along with biometric information. Secondly, an attacker cannot utilize a resetting technique, as we have mentioned in our protocol that if the attacker desires to use resetting technique, he/she first has to login into the system.

B. System Model

The proposed scheme is based on the basic assumption that the distributed mobile cloud computing environment has three basic entities: 1) mobile cloud Users (U); 2) Cloud Service Providers (CSP); 3) Token Service Provider(TSP). The system contains a set of m legal mobile cloud users, M = {Ui |i = 1, 2, . . . , m}, a set of n cloud servers, N = {CSP j|j = 1, 2, ..., n} and the trusted TSP. The authentication factors used in our scheme are: 1) Identity IDi of a user Ui ; 2) Password PWi of Ui ; 3) Biometrics Bi of Ui . The proposed scheme is composed of three phases: 1) registration; 2) login, authentication and key agreement; 3) revocation and reissue. The registration phase is composed of mobile cloud users registration phase and cloud service providers registration phase. During the registration phase, mobile cloud users and cloud service providers register to the TSP independently. The TSP generates the ZK-token for the registered servers and users. In the login, authentication and key agreement phase, the CSP first receives the user's ZK-token and verifies its authenticity. And then, the mobile user and cloud server authenticate each other and generate the secret shared session key. The revocation and reissue phase gives the flexibility for the user to update validate factors into a new password or new personal biometric characteristics for secure reasons. A legal user or an unregistered external person may execute malicious activities in the system, called as an adversary A. A mobile user can access multiple cloud service providers, and the TSP does not need to participant in the login, authentication and key agreement processes. The necessary notations list are used to design the proposed scheme. The proposed scheme makes use of the current system timestamps along with the random nonces to protect strong replay attacks.

The rest of the paper is organized as follows. In Section II the system model is proposed system. In Section III numerical simulations are presented. Finally in Section IV a conclusion is drawn.

II. LITERTURE SURVEY

Ashok Kumar Das et al [1] presented a Multi- server authentication scheme using biometrics based smart card and Elliptic Curve Cryptography (ECC). In first analyse He-Wang's scheme and show that their scheme is vulnerable to a known session-specific temporary information attack and impersonation attack. In addition, to show that their scheme does not provide strong user's anonymity. Furthermore, He-Wang's scheme cannot provide the user revocation facility when the smart card is lost/stolen or user's authentication parameter is revealed. Apart from these, HeWang's scheme has some design flaws, such as wrong password login and its consequences, and wrong password update during password change phase. We then propose a new secure multi server authentication protocol using biometric-based smart card and ECC with more security functionalities. Using the Burrows Abadi-Needham (BAN) logic, we show that our scheme provides secure authentication. In addition, we simulate our scheme for the formal security verification using the widely- accepted and used AVISPA (Automated Validation of Internet Security Protocols and Applications) tool, and show that our scheme is secure against passive and active attacks. Our scheme provides high security along with low communication cost, computational cost, and variety of security features. To show that He-Wang's scheme fails to prevent known session temporary information attack, and as a result, their scheme cannot prevent the reply attack and impersonation attack. In addition, we show that their scheme cannot provide the strong user anonymity.

Nai-Wei Lo et al [2] presented a modern societies, the number of mobile users has dramatically risen in recent years. In this paper, an efficient authentication scheme for distributed mobile cloud computing services is proposed. The proposed scheme provides security and convenience for mobile users to access multiple mobile cloud computing services from multiple service providers using only a single private key. The security strength of the proposed scheme is based on bilinear pairing cryptosystem and dynamic nonce generation. In addition, the scheme supports mutual authentication, key exchange, user anonymity, and user untraceability. From system implementation point of view, verification tables are not required for the trusted Smart Card Generator (SCG) service and cloud computing service providers when adopting the proposed scheme. In consequence, this scheme reduces the usage of memory spaces on these corresponding service providers. In one mobile user authentication session, only the targeted cloud service provider needs to interact with the service requestor (user). The trusted SCG serves as the secure key distributor for distributed cloud service providers and mobile clients. In the proposed scheme, the trusted SCG service is not involved in individual user authentication process. With this design, our scheme reduces authentication processing time required by communication and computation between cloud service providers and traditional trusted third party service. Formal security proof and performance analyses are conducted to show that the scheme is both secure and efficient.

Yuh-Min Tseng et al [3] presented A multi server architecture consisting of multiple servers provides resources and services for clients by way of open channels. Thus, a cryptographic protocol should be offered to ensure the legitimacy of both clients and servers, and to provide communication confidentiality. In the past, a large number of ID-based Mutual Authentication and key Agreement (IDMAKA) protocols have been proposed regarding this issue. Several circumstances require a revocation mechanism to revoke misbehaving/compromised clients and servers before their intended expiration dates. To do so, the existing ID-MAKA protocols generally adopt a black/white list to revoke/permit clients for access authorization. So far, no work addresses the revocation problem on servers in the sense that clients should be notified to avoid malicious services or applications provided by revoked servers. In this article, to propose the first list-free ID-MAKA protocol with an efficient revocation mechanism for multi server architectures. When compared with previously proposed protocols, our protocol possesses three main merits. First, it provides a simple revocation mechanism to solve the management problem of both compromised clients and servers. Secondly, neither clients nor servers need to keep any black/white list. Lastly, it is well suitable for mobile clients by performance analysis and experimental data

Sandip Roy et al [4] presented Secure and efficient lightweight user authentication protocol for mobile cloud computing becomes a paramount concern due to the data sharing using Internet among the end users and mobile devices. Mutual authentication of a mobile user and cloud service provider is necessary for accessing of any cloud services. However, resource constraint nature of mobile devices makes this task more challenging. It propose a new secure and lightweight mobile user authentication scheme for mobile cloud computing, based on cryptographic hash, bitwise XOR and fuzzy extractor functions. Through informal security analysis and rigorous formal security analysis using random oracle model, it has been demonstrated that the proposed scheme is secure against possible well-known passive and active attacks and also provides user anonymity. Moreover, we provide formal security verification through ProVerif 1.93 simulation for the proposed scheme. Also, we have done authentication proof of our proposed scheme using the Burrows-Abadi-Needham (BAN) logic. Since the proposed scheme does not exploit any resource constrained cryptosystem, it has the lowest computation cost in compare to existing related schemes. Furthermore, the proposed scheme does not involve registration center in the authentication process, for which it is having lowest communication cost in compare to existing related schemes.

Mohammad Wazid et al[5] presented Smart Grid (SG) technology has recently received signifilcant attention for providing intelligent and distributed electric power transmission systems. In SG, Electric Vehicles (EVs) charging becomes one of the emerging applications. However, authentication between a vehicle user and a smart meter is required so that both of them can securely communicate among each other for managing demand response during peak hours. To address the above mentioned issues,to propose a new efficient Three-factor User Authentication Scheme for a Renewable Energy based Smart Grid environment (TUASRESG), which uses the lightweight cryptographic computations such as one-way hash functions, bitwise XOR operations and Elliptic Curve Cryptography (ECC). The detailed security analysis shows the robustness of TUAS-RESG against various well-known attacks. Moreover, TUAS-RESG provides superior security with additional features, such as dynamic smart meter addition, flexibility for password and biometric update, user and smart meter anonymity, and untraceability as compared to other related existing schemes. The practical demonstration of TUAS-RESG is also proved using the widely-accepted NS2 simulation. To propose a new remote user authentication scheme for a renewable energy based smart grid environment (TUAS-RESG), which is very efficient as it only uses the lightweight cryptographic computations. In TUAS- RESG, a vehicle user can remotely authenticate to a smart meter. After mutual authentication between user and smart meter, they establish a session key for their future secure communication. The rigorous security analysis shows the robustness of TUASRESG against the existing attacks.

Aaron J Cohen et al [6] presented Implantable Medical Devices (IMDs) are man-made devices, which can be implanted in the human body to improve the functioning of various organs. The IMDs monitor and treat physiological condition of the human being (for example, monitoring of blood glucose level by insulin pump). The advancement of Information and Communication Technology (ICT) enhances the communication capabilities of IMDs. In healthcare applications, after mutual authentication, a user (for example, doctor) can access the health data from the IMDs implanted in a patient’s body. However, in this kind of communication environment, there are always security and privacy issues such as leakage of health data and malfunctioning of IMDs by an unauthorized access. To mitigate these issues, in this paper, we propose a new secure remote user authentication scheme for IMDs communication environment to overcome security and privacy issues in existing schemes. We provide the formal security verification using the widely-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. We also provide the informal security analysis of the proposed scheme. The formal security verification and informal security analysis prove that proposed scheme is secure against known attacks. The practical demonstration of the proposed scheme is performed using the broadly- accepted NS2 simulation tool. The computation and communication costs of the proposed scheme are also comparable with the existing schemes. Moreover, the scheme provides additional functionality features such as anonymity, untraceability and dynamic implantable medical device addition

III. PROPOSED SYSTEM

Figure 1.1 shows the system model of the desirable scheme for the cloud computing environment. Three parties take part in the proposed scheme: mobile cloud users, mobile cloud service providers, and a registration center. Please note that the trusted third party used in our scheme is named TSP instead of the traditional SCG or RC since our issued tokens are more widely used and do not work the same as traditional credentials. To assume that there are many mobile users and service providers within the mobile cloud services environment, and a small portion of these mobile users and service providers are malicious. Mobile cloud users, cloud service providers, and the token service provider are denoted by U = fUiji = 1; :::; ng, CSP = fCSPj jj = 1;
:::;mg, and TSP. A user can access multiple mobile cloud computing services from different service providers without the involvement of the TSP.

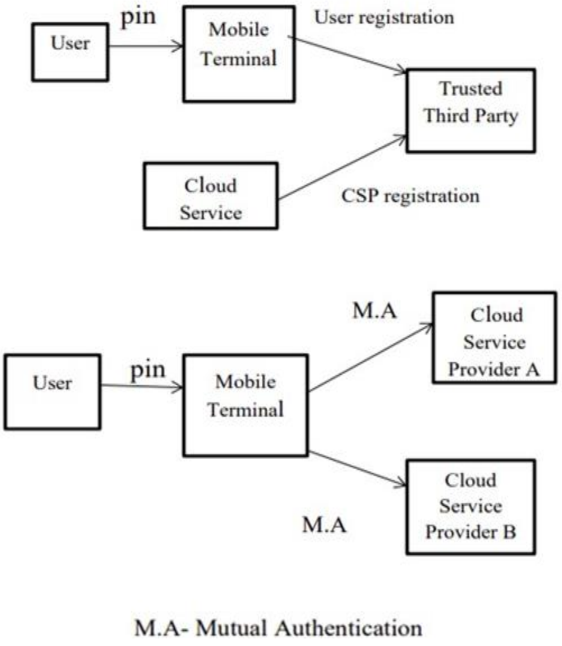


Fig.1.1 Architecture Diagram

A. Setup Phase

Initially, the Token Service Provider TSP selects a non- singular elliptic curve Ep over a finite filed GF(p). Q ∈ G is the generate point, where p is a large prime and G is an additive cyclic group of order p consisting of points on Ep. H(•) : {0, 1} ∗ → Z ∗ p is a hash function; x ∈ Z ∗ p is the secret key; PK = −xQ is the public key. The common reference string is (p, Q, PK, H(•))

B. Registration Phase

To access Cloud Service Providers (CSP), the users need to register at the TSP via a secure channel.
Registration phase of the mobile user

- In this phase, a user sends a request and obtains the ZK-Token from the TSP with authentication parameter
- User first chooses his own identity, personal password and imprints his biometric
- Mobile Terminal (MT) of user generates registration request message and submit to the TSP
- TSP picks a random number and computes hash value and then send token back to MT
- User stores ZK-Token that obtain from the TSP

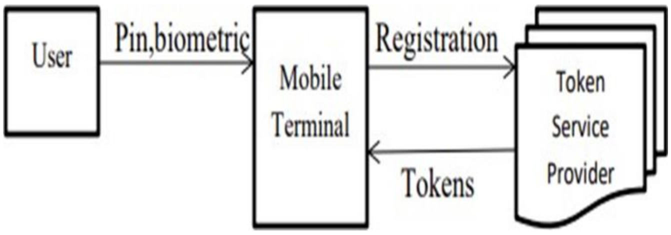


Fig.1.2 Registration Phase for Mobile user

Fig 1.2 shows the registration phase of the mobile user. In this phase, a user Ui sends a request and obtains the ZK-Token from the TSPi with authentication.
Registration phase of the CSP

- In this phase, a user sends a request and obtains the ZK-Token from the TSP with authentication parameter

- CSP first chooses his own identity IDS and select a secret
- CSP computes the registration request message and then submits to the TSP
- TSP picks a random number and computes hash value and then send token back to CSP
- User stores ZK-Token that obtain from the TSP

C. Login, Authentication and Key agreement Phase

- In this phase, CSP receives the login request message from users and two entities mutually authenticate each other.
- After successful mutual authentication, users and CSP establish a common secret session key which is used for future secure communications between them
- First, user inputs his identity ID , password PW and personal biometrics into his own mobile terminal MT
- MT use the fuzzy extractor reproduction procedure and stored signature to compute biometric secret key and hash value
- User selects a random value, computes R1 and sends K-Token and R1 to the CSP. CSP verifies hash value If failed, CSP terminates the phase.

In this phase, CSPj receives the login request message from Ui and two entities mutually authenticate each other. After successful mutual authentication, Ui and CSPj establish a common secret session key Kij which is used for future secure communications between them. The following steps needed in this phase.

D. Revocation and Reissue

- The client and server time update tokens will not be available after the time expires a2.3nd the token needs to be reissued by the token service provider.
- For client and cloud server providers, the process of updating tokens is the same as applying for tokens.

IV. RESULT AND DISCUSSION

In existing work, a Registration Server (RS) delivers a link to all the users who have performed registration successfully, and then each user uses the link to obtain and install software in their device while also providing their credentials (password, identity and biometric signature.) Note that while the password may be guessed, it is hard to guess biometric signatures. Then, the software encrypts important files by using a negotiated key to provide security on the storage file. Whenever, the user of that device wants to access that file, RS first verifies the user and then provides a decryption key to recover the original file. All the files are then encrypted using a new session key.

A. Performance Graph

In this section, give the comparison of previous proposed ID-MAKA schemes designed for mobile cloud computing services In Figure 5.1, simulated a large number of users accessing mobile cloud services and recorded the time spent on 200, 400, 600, 800, and 1000 users, respectively, without communication delay, which are 1.82s, 3.37s, 4.83s, 6.97s, 8.09s.. Compare with existing scheme, the proposed scheme saves half of time consumption,, it also does not add a lot of computational overhead.

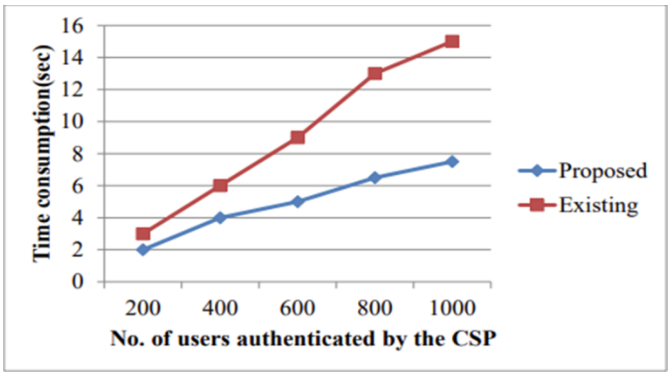


Fig 1.1 Time consumption without communication delay

For communication overhead, we concern the Number of communication rounds. Our scheme needs three communication rounds in login, authentication and key agreement phases. In Fig 1.1, we simulated a large number of users accessing mobile cloud services and recorded the time spent on 200, 400, 600, 800, and 1000 users, respectively, which are 15.80s, 33.90s, 48.34s, 70.31s, and 84.09s. Compare with Fig 1.1, we found that for all schemes, the time delay caused by communication delay is much higher than the time loss caused by the cryptographic calculation. Therefore, in the future 5G communication environment, the applicability and practicality of our scheme will be greatly enhanced.

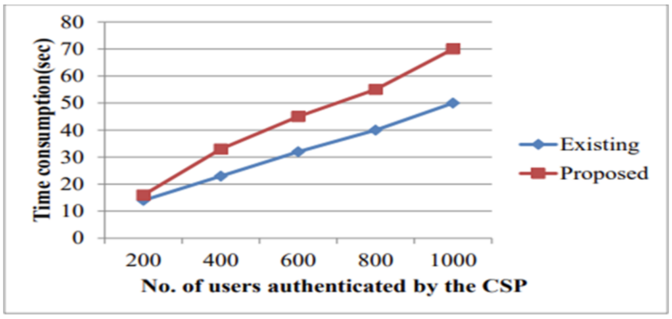
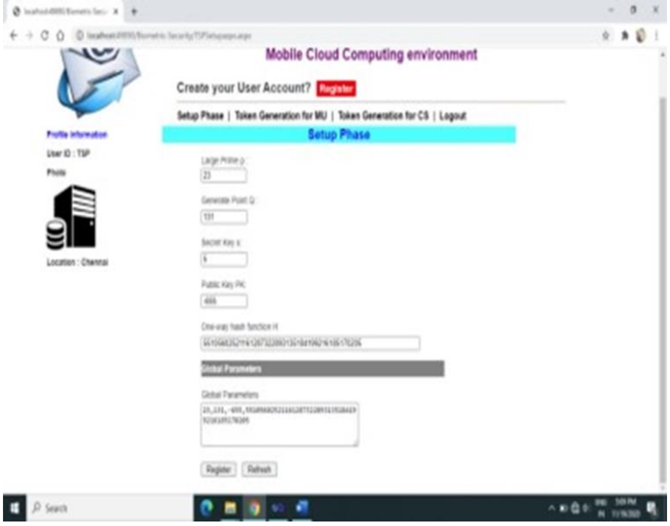


Fig 1.2 Time consumption at wireless communication internet environment

To mention the underlying cryptographic operations for each relevant scheme in comparison. To study that the total user side computation overhead of the proposed scheme in login, authentication and key agreement phases. On the other hand, the cloud service provider CSPj has a computation overhead. The average execution time. we simulated a large number of users accessing mobile cloud services and recorded the time spent. The proposed scheme saves half of time consumption, and for Roy's lightweight scheme, it also does not add a lot of computational overhead. In we tabulate and compare the communication overheads of the proposed scheme with the relevant schemes. For communication overhead, we concern the number of communication rounds. Our scheme needs three communication rounds in login, authentication and key agreement phases. we found that for all schemes, the time delay caused by communication delay is much higher than the time loss caused by the cryptographic calculation. Therefore, in the future 5G communication environment, the applicability and practicality of our scheme will be greatly enhanced.


Create your User Account?
Register
Setup Phase | Token Generation for MU | Token Generation for CS | Logout
Global Parameters
Register
Refresh
Search

Mobile Cloud Computing environment

Setup Phase

Profile Information

User ID : TSP

Photo

Location : Chennai

Large Prime p: 23

Generate Point Q: 131

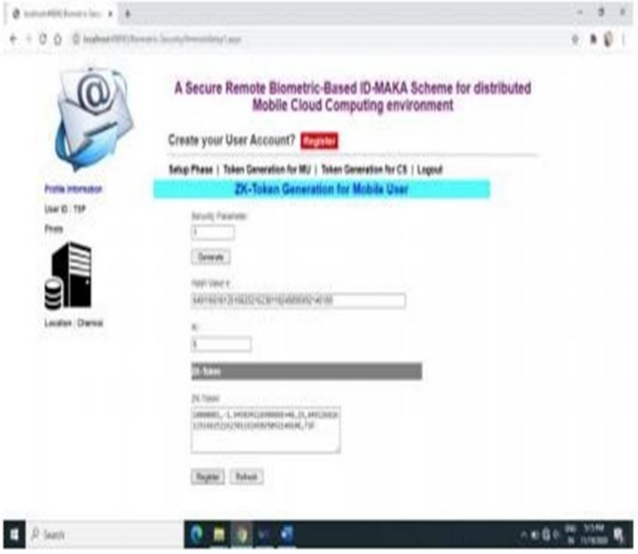
Secret Key s: 5

Public Key PK: 466

Fig 1.3 Moblie Cloud Computing Environment

A Secure Remote Biometric Based ID MAKA Scheme for distributed Mobile Cloud Computing
Finger Image

Fig 1.4 File Access


Create your User Account?
Register
Setup Phase | Token Generation for MU | Token Generation for CS | Logout
Generate
ZK Token
Register
Refresh
Search

A Secure Remote Biometric-Based ID-MAKA Scheme for distributed Mobile Cloud Computing environment

ZK-Token Generation for Mobile User

Profile Information

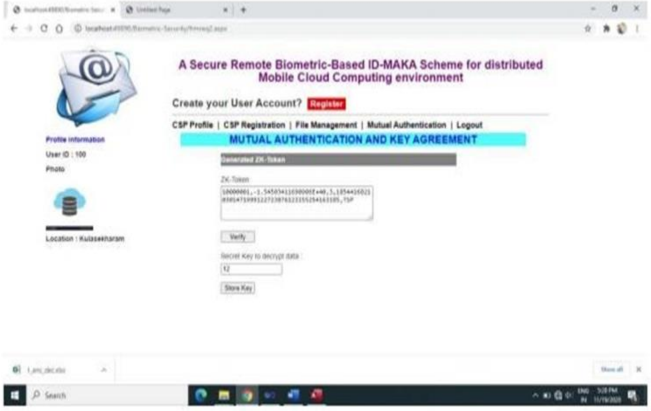
User ID : TSP

Photo

Location : Chennai

Security Parameter: 1

Fig 1.5 Generate The ZK Tokens



A Secure Remote Biometric-Based ID-MAKA Scheme for distributed Mobile Cloud Computing environment

Create your User Account? Register

MUTUAL AUTHENTICATION AND KEY AGREEMENT

Profile information

User ID : 100

Photo

Location : Kulasekharam

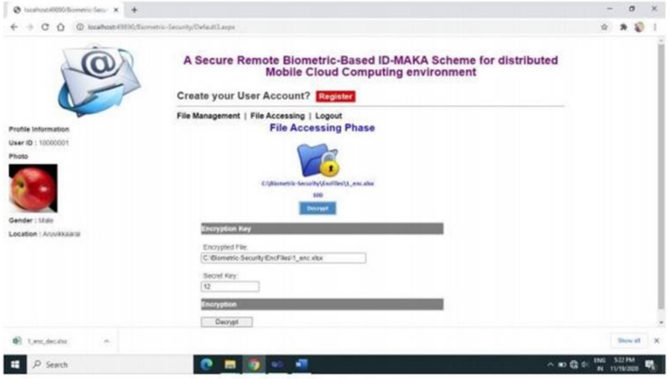
Generated ZK-Token

ZK-Token: 10000001,-1.54503411690000E+40,5,1054416021 0305471999122723876122155254163105,TSP

Secret Key to decrypt data : 12

CSP Profile | CSP Registration | File Management | Mutual Authentication | Logout
Verify
Store Key
Search

Fig 1.6 Mutual Authentication And Key Agreement



A Secure Remote Biometric-Based ID-MAKA Scheme for distributed Mobile Cloud Computing environment

Create your User Account? Register

File Accessing Phase

Profile Information

User ID : 10000001

Photo

Gender : Male

Location : Aruvikkarai

C:\Biometric-Security\EncFiles\1_enc.xlsx

100

Encryption Key

Encrypted File: C:\Biometric-Security\EncFiles\1_enc.xlsx

Secret Key: 12

Encryption

Fig 1.7 Mutual Authentication And Key Agreement

V. CONCLUSION

In this article, we propose an ID-MAKA scheme which firstly achieves biometricsbased remote authentication, single sign on, and center-less for mobile cloud computing services. We have used the Real-Or- Random model and the BAN logic for formal security analysis, and also give an additional security analysis for other known attacks. The results show that our scheme is secure from well-known possible attacks. Besides, the high privacy of our schemes much protects users' sensitive data and personal information during the authentication process. Finally, by experimental data, we demonstrate that our scheme has low computational overhead and time consumption, which is suited for the mobile cloud users with low-power computing devices. Future works: We are working on the methods of efficient token revocation and reduce the communication round. Even more, we also try to apply it to the Internet of Things.

VI. REFERENCES

[1]. Aad van Moorsel.Amjad Aldweesh Dong, . Changyu, Yilei Wang, , Patrick McCorry, and "Betrayal, Distrust, and Rationality: Smart CounterCollusion Contracts for Verifiable Cloud Computing." In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17, 211– 27. Dallas, Texas, USA: ACM Press, 2017.

[2]. Abdalla M , Fouque P A , Pointcheval D. "Password- based authenticated key exchange in the threeparty setting,[C] "// International Conference on Theory & Practice in Public Key Cryptography. Springer-Verlag, 2005

[3]. Adrijit Goswami, Ashok Kumar Das, Odelu and Vanga "A Secure BiometricsBased Multi-Server Authentication Protocol Using Smart Cards." IEEE Transactions on Information Forensics and Security 10, no. 9 (September 2015): 1953–66. https://doi.org/10.1109/TIFS .

[4]. Ashok Kumar Das, Neeraj Kumar,. "Secure Three- Factor User Authentication Scheme for Renewable- Energy-Based Smart Grid Environment." IEEE Transactions on Industrial Informatics 13, no. 6 (December 2017): 3144–53.

[5]. Athanasios V Wazid, Mohammad Mauro Conti, and. Vasilakos. "A Novel Authentication and Key Agreement Scheme for Implantable Medical Devices Deployment." IEEE Journal of Biomedical and Health Informatics 22, no. 4 (July 2018): 1299–1309.

[6]. Debiao , and D. Wang. "Robust Biometrics-Based Authentication Scheme for Multiserver Environment." IEEE Systems Journal 9.3(2015):816-823.

[7]. Dodis, , L. Reyzin , Smith,A, and Yevgeniy . "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data."

International Conference on the Theory and Applications of Cryptographic Techniques Springer, Berlin, Heidelberg, 2004

[8]. Eun Jun,Yoon, and K. Y. Yoo. "Robust biometrics- based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem." Journal of Supercomputing 63.1(2013):235-255.

[9]. Gao.C, He.D, ShenH, and Wu. L "New biometrics- based authentication scheme for multi-server environment in critical systems." Journal of Ambient Intelligence and Humanized Computing 6.6(2015):825- 834,2015.

[10]. Jia-Lun, Nai-Wei and Tsai, Lo. “A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services.” IEEE Systems Journal 9, no. 3 (September 2015): 805–15.