International Journal of Engineering Science, Advanced Computing and Bio-Technology
Vol. 6, No. 4, October – December 2015, pp. 97 - 113

Achieving Privacy Protection of Multi-factor Authentication and Access Keys in Cloud Computing

Sabout Nagaraju[1] and Latha Parthiban[2]

[1]*Department of Computer Science, Pondicherry University*

[2]*Community College, Lawspet, Pondicherry-605 008, India.*

E-mail: *nagarajus.ucc@pondiuni.edu.in* , *lathaparthiban@yahoo.com*

Abstract*: Cloud computing outsources an efficient and economical Information Technology (IT) resources to small, mid and larger-scale organizations on demand. Despite huge benefits, many organizations are still reluctant to migrate to the cloud computing due to data security and privacy concerns. As result of these top and legitimate concerns, the stakeholder's resources and services need to be protected from malicious use. Authentication is the fundamental operation to verify the legitimacy of the end users. In this article we describe an authentication scheme using multi-factors namely username and password, fingerprint biometric, secrete keys, cryptographically generated random number and one-time Resource Allocation Number (RAN). This approach provides a generalized, complete, and convenient identity verification process for remote users. Our investigated mechanism not only provides the high-secure remote authentication at lowest cost but also preserves the privacy of user credentials and access keys from the service providers and other malicious attacks. With series of experiments we illustrate that our proposed scheme is more efficient and robust towards the malicious use of customer's data in cloud.*

Keywords: *cloud computing, authentication, security, privacy, fingerprint biometrics*

1. Introduction

In many developing countries, the sectors like e-Governance, finance, digital media and health care are struggling to provide reliable, transparent, secure and efficient online IT services to their stakeholders. It is more critical and expensive to deliver these requirements and also many IT projects are failing lack of proper IT infrastructures and expertise solutions. So the enterprises can migrate to the cloud computing to strengthen their IT solutions and they can meet their customers' expectations at a fraction of cost than in-house cost. P. Mell et al. [1] reported that cloud computing is an advanced business framework for outsourcing expertise and cost-effective IT solutions. In [2], the author described various cloud services available to strengthen the customer-oriented services. Especially, the small and medium scale organizations can make use of cloud services to expand their business activities world-wide.

Despite huge benefits, many organizations are still reluctant to migrate to the cloud because it is lacking in data protection [3]. The data security and privacy of the business-critical-applications are the high-profiled concerns for enterprises in a cloud. This included a high-level of necessity to protect the enterprise sensitive data from the cloud inside and

Received: 12 May, 2015; Revised: 18 October, 2015; Accepted: 29 November, 2015

outside threats. Around the clock an enterprise can provide variety of services to the stakeholders through multiple channels. The enterprises services need to ensure the compliance regulations such as Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), National Institute of Standards and Technology (NIST) and Gramm-Leach-Bliley Act (GLBA) [4] etc. Most importantly the organization reputation brand should be protected from the damage. Therefore, the enterprises are worrying about security and privacy of the sensitive data in cloud.

In online cloud-based platforms, the stakeholder expects appropriate protection mechanisms to safeguard their key valuables. As result of protection concerns, our research facilitates the strong authentication and key management scheme which effectively validates the remote user identities and secures access keys. The major advantage of our approach is to preserves the privacy of the authentication credentials from the malicious cloud insiders and outsiders.

The following are the other key advantages of our proposed work for any cloud-depended organizations:

- Provides an efficient multi-factor fingerprint biometric authentication for data security and privacy.
- Prevents the administration sessions, sensitive information and unauthorized access.
- Effectively achieves compliance regulations.
- Protects the authentication credentials and access keys from cloud inside and outside malicious attacks.
- Organizations can gain the confidence in data access control.
- Allows the enterprises to protect their stakeholder's assets in a cloud.
- Enables the organizations to achieve present and future challenges.
- Enterprise services can cover geographically with effective multi-channels integration.
- Revenue gain for all size of business stakeholders.
- High cost of running in-house data centres can be removed.
- Can provide flexible platforms to build and bring advanced services into public.

This paper further divided into seven sections. Sections 2 presents the various problems and risks associated with the cloud-based environment. The contribution of our research is summarized in Section 3. Section 4 presents an overview of our proposed authentication scheme. Section 5 describes our proposed mechanism. Section 6 reports the feasibility of our proposed scheme. Literature reviews related with our research work are presented in Section 7. Section 8 summarizes the proposed work methodology.

2. The Problems and Risks

Today's Information and Communication Technology (ICT) management organizations are operating with high competitions, brand names, and regulated environments. Therefore, the aspects of core IT services are influenced by business considerations and compliance requirements. Innovations done so for in in-house technologies, operations and security controls have been managed inside the enterprises. Since, the cloud based functional, operational, technologies and security control aspects are managed out of the enterprises. These out of boundary aspects have highly influenced on the organization adoption and sometimes this adoption may damage trust, reputation and brand name of the organisation. As part of the threats land-space within a cloud, the enterprise online services need to be safeguard from the inside and outside malicious use. The followings are the biggest and legitimate security and privacy concerns associated with the online cloud-based platforms from the point of stakeholders. These are the problems we have envisioned in our proposed research work.

1) For some financial gain, dishonest cloud staff may steal the authentication details of the remote users from the credentials database and they may use these details for acquiring user's sensitive information.

2) User's biometric fingerprint details are unique and they may use these details for accessing more than one application. If the fingerprint details are compromised, then the users cannot change these details over the time.

3) User's personal information and activities could be tracked by using certain biometric fingerprint data.

4) In cloud computing, performing authentication process on plain credentials is not at all securable because some authentication servers may be untrustworthy.

5) Snooping user's identities could be possible in cloud environment, where the attackers may gain the users credential information transmitted over the network.

6) Make sure that the user access keys such as master keys and one-time session keys are more secured, because these keys generates less cipher text and opponent can easily work on this cipher text. Access keys for the cloud-based environment that rented out from some cloud vendors need to appropriately managed and protected.

7) Similarly, dependency on geographic or legal jurisdiction that becomes another added point to consider, because certain laws in certain political jurisdictions may allow certain local agencies unrestricted access to the data that is hosted within their territory. For instance, the patriot law in the United States allows certain US agencies to demand access to the data which is stored in the US Union Territory. Enterprises are sensitive to this kind of a situation. So, need to take appropriate measures to make sure that authentication information still remains private regardless of whether it is stored in any territory.

From the organizations perspective several risks are associated with cloud-based solutions. Some of the key risks we considered are summarized below.

i. Complexity in compliance regulations and audit management

ii. Dilution in functional, operational and technology control can leads impact on reputation, regulatory and business if service is hampered in cloud.
iii. Difficulties in sustaining security standards, regional privacy laws and information acts.
iv. Enterprise services will be locked in cloud and it is difficult to bring back in-house if required.
v. Potentially cloud API's are lacking in portability, so stakeholders cannot move from one cloud service provider to another.

3. Our Contribution

The following are the major contribution of our research.

1) Multi-factor Fingerprint biometric Authentication (MFA): The multi-factors are user ID and password, fingerprint biometric, secret keys, cryptographically generated random number and one-time Resource Allocation Number (RAN) are used as key credentials in authentication process. Where user ID and password shows what user know, fingerprint biometric represents what user are, and other credentials are used for verifying the users identity to servers and servers identity to users. The proposed MFA provides a convenient and high-secure multi-stage identity verification process for validating the authenticity of the stakeholders.
2) Protection and management of access keys: We used Station-To-Station protocol for preparing, securing and exchanging one-time session keys. Master and session keys are never stored in cloud authentication database due to privacy concerns.
3) Strong privacy preservation of user credentials: In our proposed authentication scheme, encrypted credentials are used for authentication and it allows the authentication servers to perform remote user's authentication on the hashed data.
4) In our approach login and authentication details are encrypted at rest, transit and in use.
5) The following are the major threats resolved with our proposed authentication scheme.
   i. User authentication credentials are not revealed to the malicious insiders and outsiders.
   ii. The malicious insiders of the cloud can't learn or leak the credentials of consumer's.
   iii. The mutual authentication of a user and their associated servers.
   iv. An attacker may eavesdrop on the credential communication channel and he/she may use replay attack.
   v. Sometimes, an attacker may change the network IP of the authorized user so that the request is coming from that altered system appears to be request coming from the impersonated user.
   vi. Dictionary and man-in-the-middle attacks are prevented.

6) Provable security and privacy: With the above innovations, our proposed authentication scheme provides a true protection for the user credentials in the cloud. Therefore the problems and risks envisioned in the previous section can be achieved.

4. Our Proposed Authentication Scheme

In cloud, protecting consumer credentials and access keys from the dishonest cloud staffs and other malicious users is a challenging task. As a result, we proposed an efficient privacy protection multi-factor authentication scheme. The following are the key innovations of our proposed work: (i). User can select their convenient user-id (*UID*) and password (*PWD*), and the password must include at least one digit, one control character, uppercase and lowercase letters, and one punctuation symbol quite strong. We followed the proper rules and regulations to create, lockout and reset passwords as described in [23-26]. (ii). Only the plain user-id and phone numbers are kept in cloud as shown in Table I and remaining user identification details are stored in in-house database and (iii). Hashed password, encoded and hashed biometric fingerprint data and encrypted random number are kept in the highly secured cloud authentication database.

A consumer who wants to avail a particular cloud online service needs to register with the enterprise, where customer has to submit his/her personal identification details such as permanent address proof, mobile number (*MN*), mail-id and most importantly biometric fingerprint (*BF*). Enterprise does user registration process with their cloud service providers. In this registration phase, user module takes *UID*, *PWD*, *BF* and *MN* as input from the remote user and computes the hashed password (*HPWD*) using public one-way hashing algorithm. Similarly user biometric fingerprint template is also encoded and hashed (*HBF*) using cryptographically generated random number (*RN*) and SHA-1 family respectively. The cryptographically generated random number is also encrypted by using user's fingerprint biometric data and that is indicated as *ERN*. This registration process is depicted in Figure 1. Once the registration is successful, then the registration details are sent to the user mail-id.

In login and authentication phase, user module takes *UID*, *PWD**, and *BF** as input from the remote user as shown in Figure 1. From these inputs the user-id (*UID*) will be sent to the Cloud Authentication Server (CAS) for verification. CAS verifies the *UID* and its status; if it is valid then CAS computes the secrete value and sends to the user. After receiving CAS secrete value, user module also computes the secrete value and sends to the CAS. Both user and CAS will prepare the one-time session keys for encrypting user authentication details. Here, Diffie-Hellman key exchange mechanism is used for preparing session keys. User module next computes the hashed password, then encrypts it using session key and then sends to the CAS. The CAS decrypts and obtains the hashed password using its session key, then compares the user hashed password with the cloud database hashed password, if it is matched then sends the encrypted random number (*ERN*) to the user in encrypted form using its session key. User module decrypts the cipher text using

session key and obtains *ERN*. Here, the original random number will be obtained using user biometric fingerprint, then this number will be used for encoding the user biometric fingerprint template. Finally the user module performs the hashing on the encoded fingerprint and then encrypts it with the session key and then sends to the CAS. Cloud authentication server retrieves the user hashed biometric fingerprint using it session key and performs the matching with the database hashed biometric fingerprint data. If it is matched, then the user will be allowed to access the enterprise online services from the cloud.

UID	**MN**	***p***	***g***	***Status***
UID_1	MN_1	p_1	g_1	Valid/Invalid
UID_2	MN_2	p_2	g_2	Valid/Invalid
….	….	….	….	….
UID_i	MN_i	p_i	g_i	Valid/Invalid
….	….	….	….	….

Table I. User's Non-Secrete Credentials

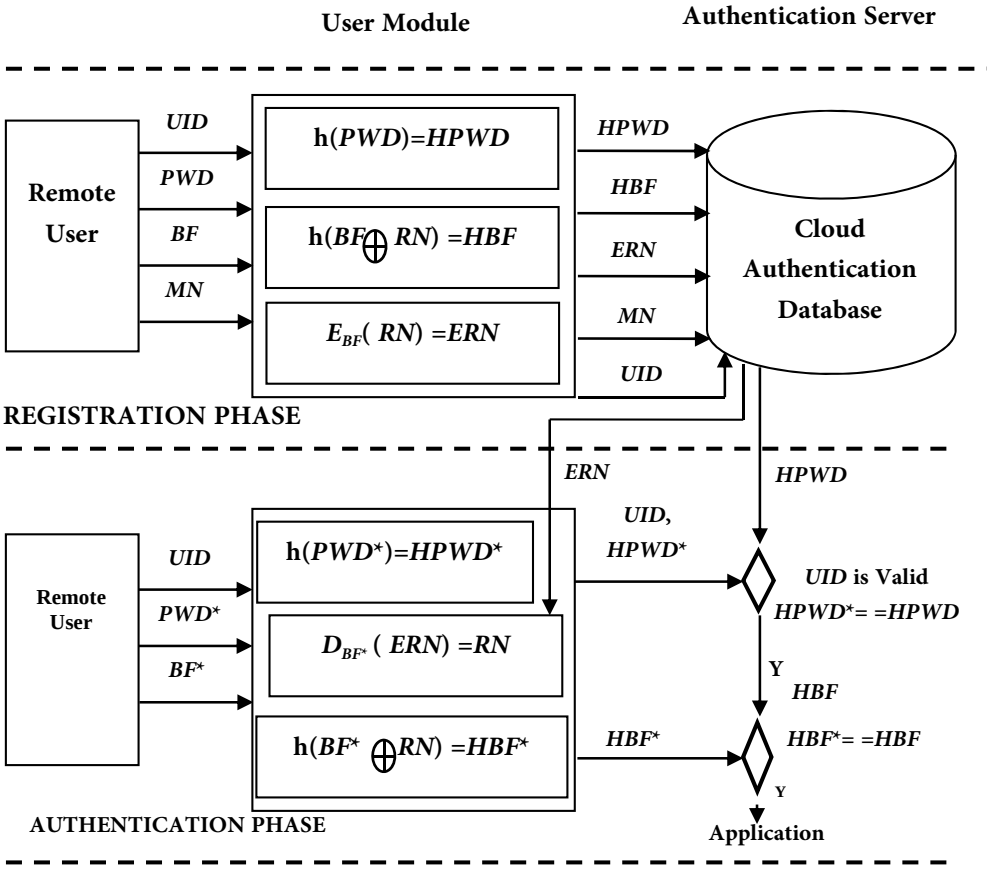

Figure 1: Block diagram of our proposed authentication scheme

Our proposed fingerprint-based authentication scheme is briefly illustrated in Figure 1. Here, the hashed password and encoded and hashed fingerprint data of each user is validated in the cloud. To describe our authentication approach, we introduce some important terminologies. We denote the registered password as *PWD*, biometric fingerprint data as *BF* and the user login password as PWD^* and fingerprint biometric data as BF^*. We represent the registered hashed password as *HPWD*, and encoded and hashed biometric fingerprint data indicated as *HBF*. The user login hashed password denoted as $HPWD^*$ and encoded and hashed fingerprint biometric data indicated as HBF^*. Further we use Δ as a matching algorithm for checking correctness of the hashed biometric data, and the function $\boxtimes_{RN}$ with random number *RN* is used for encoding fingerprint biometric data using *exclusive OR* operation. The function $\boxtimes_{RN}$ cannot be computationally reversible without *RN* and will not affect on Δ matching results. The user module sends $h(PWD^*)$ and $h(\boxtimes_{RN}(B^*))$ to the *CAS* for authentication. The CAS checks $h(PWD^*)=h(PWD)$ and matches $\Delta\ (HBF, HBF^*) = (h(\boxtimes_{RN}(BF)), h(\boxtimes_{RN}(BF^*))$. Thus, *CAS* cannot learn the original password and fingerprint biometric data, but still it can evaluate the correctness of the user credentials.

5. Completeness of our Scheme

In this section we describe our privacy protected multi-factor authentication approach, in which consumer registration and authentication will be performed using following three phases.

Initialization phase, the cloud authentication server chooses a larger prime value for *p*, where *p* contains at least 300 digits and selects a primitive root value for *g*, where *g* need not be larger. The *p* and *g* values will be used in login and authentication phase for preparing secrete session keys.

In registration phase, consumer registers with the enterprise and cloud authentication database as follow.

1) A user U who wants to avail the enterprise cloud online services must produce a valid personal identity, mobile number and mail-id at the enterprise. In this process, the user needs to choose a user-id and password where user selected password strength will be evaluated using the strong password checker and then need to pick a random secrete key '*SK*'. Finally, the user fingerprint will be captured using high resolution scanners and creates a biometric fingerprint template. Thus the client module computes $h(PWD)$, here $h(.)$ indicated as one-way hash function, $HBF= h(\boxtimes_{SK}(BF))=h((SK \oplus BF))$, and $E_{BF}(SK)$, where $E_{BF}(.)$ is a symmetric encryption function.
2) Client module sends *UID*, *HPWD*, *HBF*, *and ESK* to the CAS through highly secured internet channel.
3) The CAS stores *UID*, *MN*, *p*, *g* and their *status* in one table as shown in Table I, where *status* denotes whether the registered *UID* is unrevoked or not and other credentials are

stored in password and biometric fingerprint tables. All these tables are kept in a highly secured cloud authentication database.

4) Cloud authentication server sends the registration details to the user mail-id.
5) The login and authentication phase, takes the following steps for validating correctness of the end user credentials.
   1) In login page, a random string (*RS*) is generated for encrypting *UID*.
   2) User enters *UID* and password PWD^*, then user module computes the cipher text $C_0 = E_{RS}(UID)$ and sends to the CAS.
   3) The CAS decrypts C_0 using a random string *RS* and obtains user-id *UID*, and then checks the *UID* in the non-secrete credentials table, if it found and valid, then CAS chooses a secrete number X_A (X_A < p) and computes $Y_A = g^{X_A} \bmod p$ and sends ($Y_A \,||\, p \,||\, g$) to the user module. Otherwise the login request will be rejected.
   4) User module also selects a secrete number X_B (X_B < p) and computes $Y_B = g^{X_B} \bmod p$ and sends Y_B to the CAS.
   5) Then after both user module and CAS finds their shared secretes (*SS*).
   6) User module computes the hashed password as HPWD*=h(PWD*), where *h*(.) indicated as one-way hash function and encrypts it with *SS* as $C_1 = E_{SS}$(HPWD*), where E_{SS}(.) is a symmetric encryption function and sends to the CAS.
   7) CAS decrypts C_1 as $P_1 = D_{SS}(C_1)$ using its shared secrete and then checks $HPWD^* == HPWD$. If both the passwords are equivalent, then *CAS* sends *ESK* (i.e., $\boxtimes_{BF}(SK)$) to the user in encrypted form as $C_2 = E_{SS}(ESK||OTSK)$, where *SS* is shared secrete. Otherwise the login request will be rejected.
   8) User module asks for user biometric fingerprint.
   9) User submits biometric fingerprint *BF** to the user module.
   10) User module retrieves (ESK||*OTSK*) by decrypting C_2 using shared secrete, where *OTSK* is CAS one-time symmetric key. User module also obtains the secrete key *SK* using user biometric fingerprint data BF^* as $SK = A(\boxtimes_{BF}(SK), BF^*)$, where A(.) is a extracting function corresponding to $\boxtimes_{BF}(.)$. The user then computes $HBF^* = h((\boxtimes_{SK}(BF^*))) = h((SK \bigoplus BF^*))$ and derives $C_3 = E_{OTSK}(HBF^*)$ and sends C_1 to the CAS.

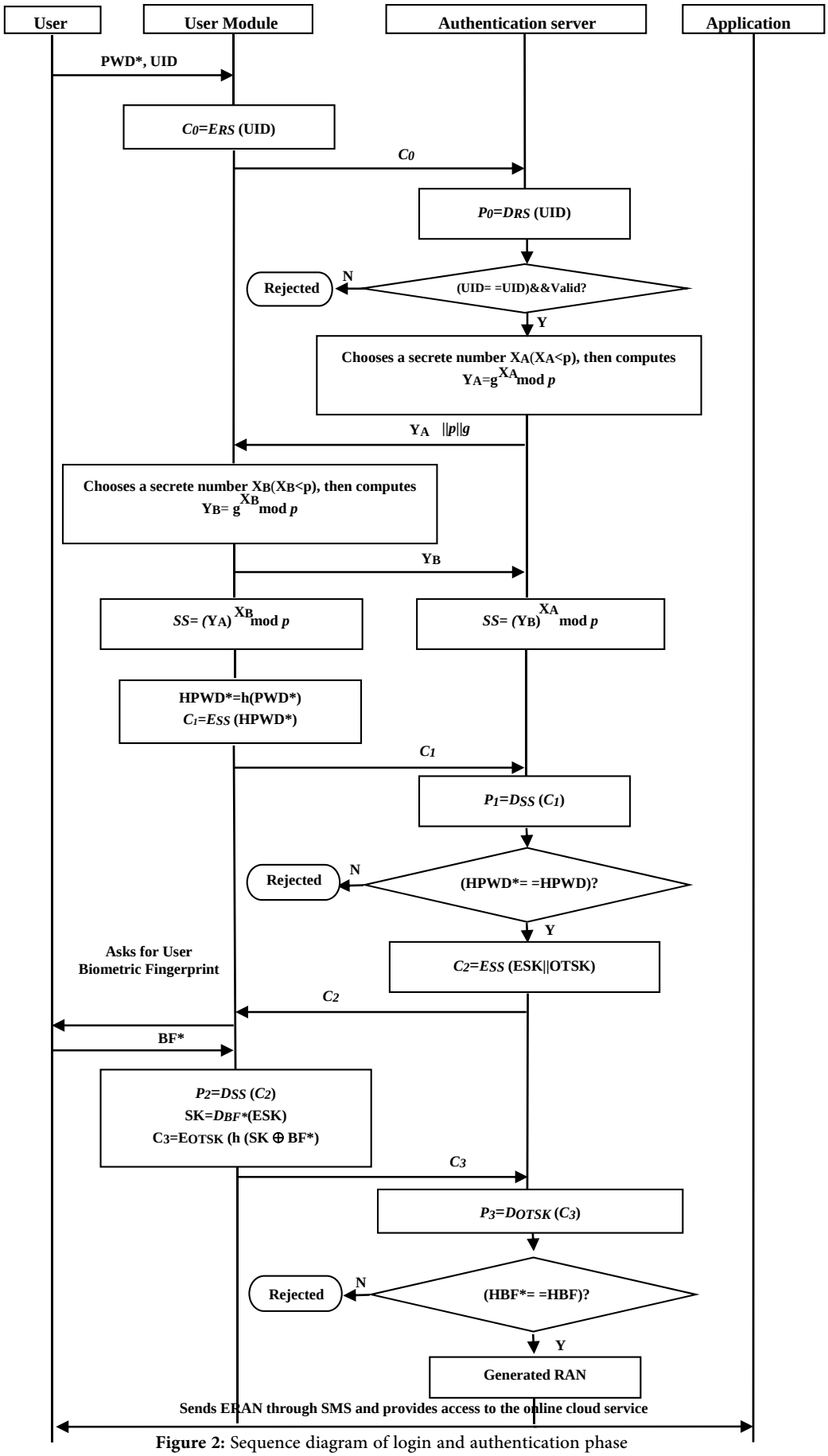

Figure 2: Sequence diagram of login and authentication phase

1) Finally, the cloud authentication server obtains hashed biometric fingerprint data as $HBF^{\star}=P_3=D_{OTSK}(C_3)$ and performs matching function on P_3 i.e., $\Delta(HBF, HBF^{*}) = (\boxtimes_{SK}(BF), \boxtimes_{SK}(BF^{*})$ and checks the matching score whether it is greater than or equal to a predefined threshold. If it is true, then *CAS* decides that the request has come from the authorized user and sends one-time unique Resource Allocation Number (*RAN*) to the user registered mobile number through SMS. The user can use this *RAN* for accessing enterprise service from cloud. The sequence diagram of login and authentication phase is represented in Figure 2.

6. Experimental Evaluation

The objective of this section is to report the feasibility of our proposed privacy protection authentication mechanism. Before presenting the performance evaluation of our proposed work, we present the experimental setup including login and fingerprint databases we used. We describe the performance and properties of our multi-factor biometric fingerprint authentication scheme in terms of security, time taken for login and authentication process, etc. With the extensive analysis and experiments we show that our proposed mechanism not only provides the strong authentication, but also achieves the privacy of the credentials and access keys.

A. Experimental Setup

Setup: We implemented our framework in C#.NET framework using Visual Studio community 2013 and SQL Server 2012 R2 SP1. We use a machine running windows 8.1 64-bits with 4GB RAM, 2.0GHz Intel Core i7 processor, and a fingerprint reader. We used Elliptic Curve Cryptosystem [11] for public-key encryption/ decryption.

Databases: We use four disjoint fingerprint databases (*FDB*'*s*) which taken from FVC2006 database [12]. Each *FDB* images are captured using four different sensors details are given in Table II with the cooperation of 150 heterogeneous participants includes industrial, academic and elderly people. Each *FDB* contains 150 fingers and in-depth 12 samples per finger (i.e., 150x12=1800). Samples were of exaggerated distortion, dry/wet impressions and large amount of displacement and rotations. Each *FDB* is divided into two disjoint sub-databases as follow:

1. FDB1-A, FDB2-A, FDB3-A, and FDB4-A, where each sub-databases stores 140 fingerprint samples of their corresponding *FDB*.
2. FDB1-B, FDB2-B, FDB3-B, and FDB4-B, where each sub-databases stores ten fingerprint samples of their corresponding *FDB*.

Where, B sub-databases contain the most difficult fingerprint images used for evaluating protection strength of the proposed scheme. We generated 150 *UID*'s and *PWD*'s using GNU-licensed open source data generator tool [13].

Data base	Sensor Type	Resolution	Image Size
FDB1	Optical	569 dpi	400x560(224Kpixels)
FDB2	Electric Field	250 dpi	96x96(9Kpixels)
FDB3	Thermal sweeping	500 dpi	400x560(200Kpixels)
FDB4	SFinGe v3.0	500 dpi	288x384(108Kpixels)

Table II: Details of Sensors used for Capturing Databases

B. Performance of our authentication scheme

First we compare our scheme with password-based and other biometric authentications in terms of computational cost. Next, we illustrate the performance of our fingerprint-based authentication mechanism.

In general, the traditional password-based authentication is more computationally effective than the fingerprint biometric-related authentication, because additional computation power is required for validating fingerprint biometric samples. To develop the multi-factor authentication with fingerprint biometric in a more practical way, the fingerprint samples related computations should be accurate and take less time. In [14], authors pointed out that the practical requirements satisfaction of the fingerprint biometric is more than other types of biometrics (e.g., iris, face, etc.) in terms of authentication and extraction (e.g., fingerprint recognition included in laptop, ATM's, PC mouse etc.).

C. Comparisons

We took Elliptic Curve Cryptosystem [11] for public-key encryption/decryption and it takes only one modular multiplication for encryption. In our approach, for each user requires four symmetric encryption/decryption, four modular multiplications, two exclusive-OR and four hash operations in the login and authentication process. Solutions [19, 21] requires minimum of two modular exponentiations for each user. In our protocol, a new idea is proposed where the user is allowed to select a user-id (*UID*) and password, not decided by the cloud credential server, so that user can memorize their *UID* and password easily. In [18, 22] mechanisms authentication servers decides UID's and passwords for remote users. The solutions [18, 20] are the timestamp based, where the clock synchronization is required between the user and server computers, and the login message transmission delay time also limited. In our approach we used the nonce to eliminate the transmission and clock synchronization delay times and also avoids masquerade, eavesdrop and other replay attacks. In [18, 20 and 21] authors do not consider the phishing, Distributed Denial-of-Service (DDoS), man-in-the browser and cross-site attacks. Our proposed authentication framework not only performs the credentials validation in *CAS*,

but also provides the login and authentication credentials privacy. Mechanisms proposed in [18-19, and 22] are not suitable for accessing sensitive online services in the cloud. Table III provides the performance comparisons of our approach with other mechanisms.

	C1	C2	C3	C4	C5	C6
A.Jyoti Choudhury et al. [18]	YES	NO	NO	NO	NO	NO
Ping Wang et al [19]	NO	YES	YES	YES	YES	NO
B.Rohitash Kumar et al [20]	YES	YES	NO	NO	NO	YES
Wenyi Liu et al. [21]	YES	YES	YES	NO	NO	YES
Hong Liu et al. [22]	NO	NO	YES	YES	YES	NO
Our Approach	YES	YES	YES	YES	YES	YES

Table III. Performance Comparison

C1: Requires low computation cost.
C2: The user is allowed to select a user-id (*UID*) and password, not decided by the cloud server.
C3: The clock synchronization is not required between the user and server computers.
C4: Robust towards phishing, Distributed Denial-of-Service (DDoS), man-in-the browser and cross-site attacks.
C5: Not only performs the credentials validation in the *CAS*, but also provides the login and authentication credentials privacy.
C6: Suitable for accessing enterprise sensitive online services in the cloud.

To the best of our knowledge, our approach is an efficient multi-factor fingerprint biometric authentication approach which provides fingerprint biometric security and privacy in a cloud-based environment.

A. Results

We validated the correctness performance of our proposed fingerprint-based authentication protocol using series of experiments with combination of 150 *UID*'s and *PWD*'s, and four FVC2006 fingerprint databases. We set the different time window bounds on FVC2006 databases for matching the correctness of given fingerprints in terms of False Negative Rate (FNR) and False Positive Rate (FPR). The false negative rate means the rate of genuine match or rejection of genuine claims and was calculated as $t_p/(t_p+f_n)*100\%$, where f_n is the total number of false negative and t_p is the total number of true positive. The false positive rate means the rate of impostor match or acceptance of impostor claims and was computed as $t_n/(t_n+f_p)*100\%$, where t_n considered as the total number of true negative and f_p taken as the total number of false positive. The recognition performance of our proposed approach for FVC2006 databases is reported in Figure 3.

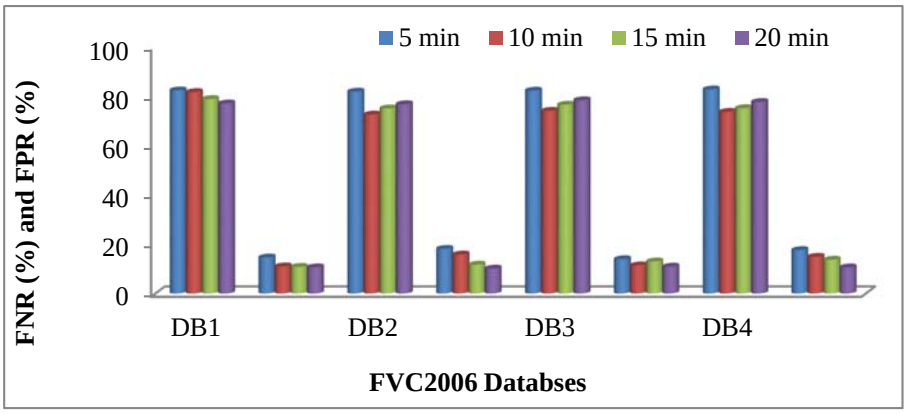

Figure 3: Our proposed approach recognition performance

We find out the Rejection Enrollment (RE), Rejection Matching (RM), Average Enrollment Time (AET), Average Matching Time (AMT), Equal Error Rate (EER) and Revised EER (REER) over the FVC2006 databases as shown in Table IV. The EER, we consider as a unit of measure of fingerprint recognition performance and it denotes where the FNR and FPR are equal. The average EER of our mechanism for the FVC2006 databases is 2.25%. From the Table IV we can understand that the EER little varies for each input fingerprint database of different sensor type. For example, the FDB4 has more equal error rate (i.e., 2.36%) compare to FDB1 EER value (i.e., 2.14%) because these two databases differ in resolution and image sizes. In our approach we got the EER and REER values are same.

Data base	EER	REER	RE	RM	AET	AMT
FDB1	2.14%	2.14%	0.00%	0.00%	1.47 s	0.21 s
FDB2	2.28%	2.28%	0.00%	0.00%	1.58 s	0.20 s
FDB3	2.23%	2.23%	0.00%	0.00%	1.74 s	0.17 s
FDB4	2.36%	2.36%	0.00%	0.00%	1.87 s	0.23 s
Avg.	2.25%	2.25%	0.00%	0.00%	1.66 s	0.20 s

Table IV: Performance of our Approach on the Four FVC2006 Databases

7. Related Work

Developing an efficient multi-factor authentication and key management approach for cloud-based platform is an open problem. Very few literatures are exists as a part of this problem in recent years. Our related work is divided into two parts; first we present the

various traditional authentication mechanisms and next we report cloud-based authentication approaches.

Several traditional multi-factor authentication approaches have been designed to integrate the fingerprint biometrics with smart-card and /or password authentication. In [5], Lee et al. developed a user identity verification approach through smart cards, where the registered user supplies their fingerprint biometric samples and password in login process. In this scheme password tables are not required, but fingerprint and smart-card tables are required for validating the user's identities. However, this mechanism was broken by the authors of [6] and [7]. In [6] pointed out that Lee's authentication approach cannot protect conspiring attack. Lin et al. [7] discovered that an authorized user can make any number of fake valid credentials to masquerade other authorised users. Lin et al. [7] discovered a scheme that maps the password and fingerprint into super password and enables authorized users to the password off-line. This approach cannot resist an impersonation attack [15]. Yoon et al. [15] presented a solution to resist this attack. This improved solution was broken by Lee et al. [16] and they made further enhancement in this scheme. This solution is not broken till now, but it failing in checking some biometrics at server side. A MFA privacy preserving protocol has been proposed by Bhargav et al. in [17] using multi-factors namely password, a random string and a fingerprint. In this scheme they formed a cryptographic key by using multi-factors for identity verification. The problem with this scheme is in authentication phase each user needs to find expensive modular exponential computations. The above traditional multi-factor authentication mechanisms, however, do not suitable for cloud-based environment and the approaches of [5-7], [15] and [16] do not considered the privacy of the user credentials.

In recent years some cloud-based authentication mechanisms have been proposed for validating user credentials. A.J. Choudhury et al. [18] presented an authentication framework to integrate the user *ID* and password with smartcard. This scheme is not enough strong for enterprises to protect intellectual properties, because it can easily compromise to replay and man-in-the-middle attacks. In [19], Ping Wang et al. described a secret-splitting authentication method for enhancing cloud security using smart-card. In this approach user id, password and one part of the encrypted biometric fingerprint data are stored in a smart-card and another part of the encrypted fingerprint template will be stored in the cloud database for user authentication. This approach preserves the credential and access keys privacy in the cloud, but it is not suitable for accessing cloud online services. Rohitash Kumar B et al. [20] proposed a *MFA* framework using the *OTP* and *IMEI* number as authentication secretes. In [21], W. Liu et al. described a multi-factor cloud authentication approach using user password and secure user profile. However, the schemes [20] and [21] reveal the user credentials to the cloud insiders and not suitable to achieve our problems, because here authors do not considered the privacy of the user credentials. Hong Liu et al. [22] discovered a privacy-preserving authentication scheme based on the shared authority details for data sharing. This theoretically proved approach helps for multi-user

collaborative applications. To address our problems stated in Section 2, the user credentials and access keys should not reveal to any cloud malicious insiders and outsiders. Our proposed fingerprint-based authentication scheme achieves the security and privacy concerns related to the remote user credentials and access keys in an online cloud services.

8. Conclusion

Cloud Computing provides the flexible, integrated and sustainable IT solutions for all size of enterprises to boost up their productivity and reduce operational cost at a fraction of the cost than in-house solution. In cloud, data security and privacy are the high profiled concerns for enterprises. This includes the protection of business-critical-applications data from malicious use. Our scheme helps significantly to strengthen the remote authentication in cloud and effectively protects the enterprises sensitive information from inside and outside malicious attackers. In our approach, the fingerprint biometric is a key parameter for authentication. Specifically the user credentials are never revealed to dishonest cloud insiders, cloud authentication servers and any other outside attackers, but allow the cloud authentication servers to perform credentials validation on the encrypted values. Therefore, the cloud malicious insiders and outsiders cannot learn or leak the authentication credentials.

References:

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," 2011. [Online]. Available: http://csrc.nist.gov /publications/nistpubs/800-145/SP800-145.pdf

[2] Abhinav Garg, "Cloud Computing for the Financial Services Industry", Sapient global markets White Papers, pp.1-16, 2011.

[3] iSMG, "Overcoming the Apprehension of Cloud Computing," 2012. [Online]. Available: http://docs.ismgcorp.com/files/ handbooks/Cloud-Survey-2012/Cloud Survey Report 2012.pdf

[4] "Best Practices for Protecting Content and Information in the Cloud", Cipher Cloud White Papers, pp.1-11, 2013-14.

[5] J. K. Lee, S. R. Ryu, and K. Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," Electron. Lett., vol. 38, no.12, pp. 554–555, 2002.

[6] C. C. Chang and I. C. Lin, "Remarks on fingerprint-based remote user authentication scheme using smart cards," *ACM SIGOPS Operating Syst. Rev.*, vol. 38, no. 4, pp. 91–96, 2004.

[7] C. H. Lin and Y. Y. Lai, "A flexible biometrics remote user authentication scheme," Comput. Standards Interfaces, vol. 27, no. 1, pp. 19–23, 2004.

[8] Antonio San Martino and Xavier Perramon, "A Model for Securing E-Banking Authentication Process: Antiphishing Approach", Proceedings of the 2008 IEEE Congress on Services, pp,251-254, 2008.

[9] Bei Guan, Yanjun Wu and Yongji Wang, "A Novel Security Scheme for Online Banking Based on Virtual Machine", Proceedings of the 2012 IEEE Sixth International Conference on Software Security and Reliability Companion, pp.12-17, 2012.

[10] Mahmoud Mohammed Mahmoud Musleh, Ismail Idrissa Ba, Karama M.A. Nofal, Jamaludin Ibrahim, "Improving Information Security in E-Banking by Using Biometric Fingerprint", Proceedings of the International Journal of Computer Science and Information Security, Vol. 10, No. 3, pp.7-12, March 2012.

[11] V. Miller, "Uses of elliptic curves in cryptography," Advances in Cryptology—Crypto85, ser. Lecture Notes in Compute Science, no. 218, pp.417–426, 1985, Springer-Verlag.

[12] R.Cappelli, M.Ferrara, A.Franco, D.Maltoni, "Fingerprint verification competition 2006", Biometric Technology Today, vol.15, no.7-8, pp.7-9, Augest 2007. http://atvs.ii.uam.es/fvc2006.html.

[13] http://www.data-generator.com/.

[14] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, "Biometric Cryptosystems: Issues and Challenges," Proc. IEEE, Special Issue on multimedia Security for Digital Rights Management, vol. 92, no. 6, pp. 948-960, June 2004.

[15] E. J. Yoon and K. Y. Yoo, "A new efficient fingerprint-based remote user authentication scheme for multimedia systems," in 9th Int. Conf. Knowledge-Based & Intelligent Information & Engineering Systems (KES 2005), 2005, pp. 332–338, Paper LNAI 3683.

[16] Y. Lee and T. Kwon, "An improved fingerprint-based remote user authenticationscheme using smart cards," in Proc. ICCSA 2006, vol. 3981, pp. 915–922, Lecture Notes in Computer Science.

[17] A. Bhargav-Spantzel, A. C. Squicciarini, E. Bertino, S. Modi, M. Young, and S. J. Elliott, "Privacy preserving multi-factor authentication with biometrics," J. Comput. Security, vol. 15, no. 5, pp. 529–560, 2007.

[18] Amlan Jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim, Hoon Jae-Lee, "A Strong User Authentication Framework for Cloud Computing", 2011 IEEE Asia -Pacific Services Computing Conference, pp. 110-115, 2001.

[19] Ping Wang, Chih-Chiang Ku and Tzu Chia Wang, "a new fingerprint authentication scheme based on secret-splitting for enhanced cloud security", Recent Application in Biometrics, pp. 183-196, July 2011.

[20] Rohitash Kumar Banyal, Pragya Jain, Vijendra Kumar Jain, "Multi-factor Authentication Framework for Cloud Computing", 2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation, pp.105-110, 2013.

[21] Wenyi Liu, A. Selcuk Uluagac, and Raheem Beyah, "MACA: A Privacy-Preserving Multi-factor Cloud Authentication System Utilizing Big Data", 2014 IEEE INFOCOM Workshops: 2014 IEEE INFOCOM Workshop on Security and Privacy in Big Data, pp. 518-523, 2014.

[22] Hong Liu, Huansheng Ning, Qingxu Xiong, Laurence T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 1, January 2015.

[23] http://www.thegeekstuff.com/2008/06/the-ultimate-guide-for-creating-strong-passwords/.

[24] https://www.microsoft.com/security/pc-security/password-checker.aspx.

[25] http://www.microsoft.com/security/online-privacy/finances-rules.aspx.

[26] Overcoming Security, Privacy & Compliance Concerns, White Paper, www.ciphercloud.com, pp.1-13, 2013.