International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Enhanced two Factor Authentication and Authorization Technique to Secure Data in Cloud

Mohd Azheruddin Adil[1], Md Ateeq Ur Rahman[2]
[1]M.Tech Scholar, Department of Computer Science & Engineering, Shadan College of Engineering & Technology, Hyderabad, Telangana, India
[2]Professor, Department of Computer Science & Engineering, Shadan College of Engineering & Technology, Hyderabad, Telangana, India

ABSTRACT

There are numerous techniques available to provide authentication level security to the various applications over a cloud. A more secure route is to utilize two-factor validation (2FA). 2FA is exceptionally regular among online e-keeping money administrations. Notwithstanding a username/secret key, the client is additionally required to have a gadget to show a one-time password. A few frameworks may require the client to have a cell phone while the one-time secret key will be sent to the cell phone through SMS amid the login procedure. By utilizing 2FA, clients will have more confidence to utilize shared PCs to login for online e-keeping money administrations. For a similar reason, it will be smarter to have a 2FA framework for clients in the online cloud benefits keeping in mind the end goal to build the security level in the framework. To Ensure Application and Data Security is the main objective of this paper. Data Owners gets verified every time by using 2FA technique for login or downloading any data. This process of authentication guarantees high level security to the application from anonymous users on the web.

Keywords : Authentication, Authorization, Two Step Verification, Second Step Validation, Secure Message Sending, Secure Authentication, Data Encryption.

I. INTRODUCTION

Distributed computing is a virtual host PC framework that empowers ventures to purchase, rent, offer, or disperse programming and other computerized resources over the web as an on-request benefit. It never again relies upon a server or various machines that physically exist, as it is a virtual framework. There are numerous utilizations of distributed computing, for example, data storage, huge data administration, medicinal data framework and so forth. End clients get to cloud-based applications through a web program, thin customer or portable application while the business programming and client's information are put away on servers at a remote area. The benefits of electronic distributed computing administrations are tremendous, which incorporate the simplicity of openness, diminished expenses and capital uses, expanded operational efficiencies, adaptability, flexibility and prompt time to showcase. the new worldview of distributed computing gives incredible favorable circumstances, there are then likewise worries about security and protection particularly for electronic cloud administrations. As touchy information might be put away in the cloud for sharing reason or helpful access; and qualified clients may likewise get to the cloud framework for different applications and administrations, client verification has turned into a basic part for any cloud framework. A client is required to login before utilizing the cloud benefits or getting to the delicate information put away in the cloud. There are two issues for the conventional record/secret key based framework.

First, the conventional record/secret word-based verification isn't security safeguarding. In any case, it is all around recognized that protection is a fundamental element that must be considered in distributed computing frameworks.

Second, it is normal to share a PC among various individuals. It might be simple for programmers to introduce some spyware to take in the login secret word from the web-program. When we consider the

previously mentioned second issue on electronic administrations, it is normal that PCs might be shared by numerous clients particularly in some huge organization or associations. For instance, let us consider the accompanying two situations:

1. In a hospital facility, PCs are shared by various staff. Dr. Alice utilizes the PC in room A when she is on obligation in the daytime, while Dr. Bounce utilizes a similar PC in a similar room when he is on obligation around evening time.
2. In a college, PCs in the undergrad lab are typically shared by various staff. In these cases, client mystery keys could be effectively stolen or utilized by an unapproved party. Despite the fact that the PC might be bolted by a secret key, it can even now be potentially speculated or stolen by undetected malwares.

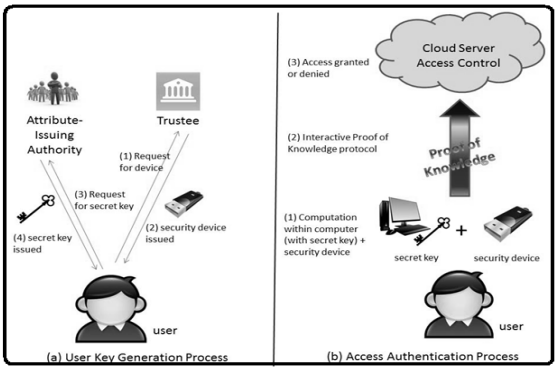


Figure 1. Proposed system framework

II. SYSTEM ANALYSIS

2.1 Introduction

We audit some related works including data based cryptosystems and access control with security gadget in this area.

Existing System:

In Every application the major authentication process for user to access application is by using credentials. In this a user has to enter his/her username and password in combination, if it matches with the existing database then the user is considered as authenticated user or else anonymous user. This process of authentication failed in major application. as one system can be used by many users for organizational work or task thus a user may lose his/her credentials here. Application never authenticates a user based on his/her identity but in very rare cases. It uses combination of two parameters irrespective of genuine user.

2.1.1 Disadvantages of Existing System:

1. User may lose his/her credentials very easily as single system is accessible for multiple users in many organization.
2. A Pair of username and password cannot be used to judge or authenticate a user.
3. There exist many techniques to authenticate a user in spite of a login form with pair of attributes.
4. First, the traditional account/password-based authentication is not privacy-preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems.
5. Second, it is common to share a computer among different people. It may be easy for hackers to install some spyware to learn the login password from the web-browser.
6. In existing, even though the computer may be locked by a password, it can still be possibly guessed or stolen by undetected malwares.

2.2 Proposed System:

In this paper we propose a novel security algorithm called as 2FA with a pair of secret key and a light weight device in combination. Implementation of two factor authentication provides application security to the next level. Basically, our proposed system works after the user is authenticated I.e. first user needs to provide his/her credentials which is a set of username and password for login in to the application. After successful login the next authentication process is called two factor authentications or second step verification. In this a user will receive a secret key on his/her device which is registered with the server. If user enters the correct secret key which they receive then they can access the entire application at that time. This technique is adopted by google Gmail service and other applications are also integrating and adopting this technique. This technique is first of its kind when implemented in cloud for security of the user and their data which is located on a remote server. Always the cloud servers are untrusted because users don't have physically interaction with it. To integrate the security and to provide trustworthy to cloud server we introduce

this 2FA scheme. Which is far more better when compared with all other schemes including captcha.

2.2.1 Advantages of Proposed System:

1. Our protocol provides a 2FA security
2. Our protocol supports fine-grained attribute-based access which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is also preserved.

III. METHODOLOGY

A. Property Based Cryptosystem Attribute-based encryption (ABE) is the foundation of quality based cryptosystem. ABE empowers fine-grained get to control over encoded information utilizing access approaches and connects qualities with private keys and ciphertexts. Inside this unique situation, ciphertext-approach ABE (CP-ABE) permits an adaptable method for information encryption with the end goal that the encryptor defines the entrance arrangement that the decryptor (and his/her traits set) needs to fulfill to decode the ciphertext. Accordingly, extraordinary clients are permitted to unscramble distinctive bits of information regarding the pre-defined strategy.

This can wipe out the trust on the capacity server to counteract unapproved information get to. Other than managing verified access on scrambled information in distributed storage benefit, ABE can likewise be utilized for get to control to distributed computing administration, comparatively as an encryption plan can be utilized for validation reason: The cloud server may encode an arbitrary message utilizing the entrance strategy and request that the client decode. In the event that the client can effectively decode the ciphertext (which implies the client's characteristics set satisfies the endorsed approach), at that point it is permitted to get to the distributed computing administration. Notwithstanding ABE, another cryptographic primitive in trait based cryptosystem is characteristic based mark (ABS). An ABS plot empowers a client to sign a message with fine-grained control over distinguishing data. Specifically, in an ABS plot, clients get their quality private keys from a characteristic expert. At that point they can later sign messages for any predicate satisfied by their qualities. A verifier will be persuaded of the way that the underwriter's characteristics fulfill the marking predicate if the mark is substantial. In the meantime, the personality of underwriter stays covered up. In this manner, it can accomplish mysterious property based access control efficiently. As of late, Yuen et al. proposed a characteristic based access control instrument which can be viewed as the intuitive type of ABS.

B. Access Control with Security Device

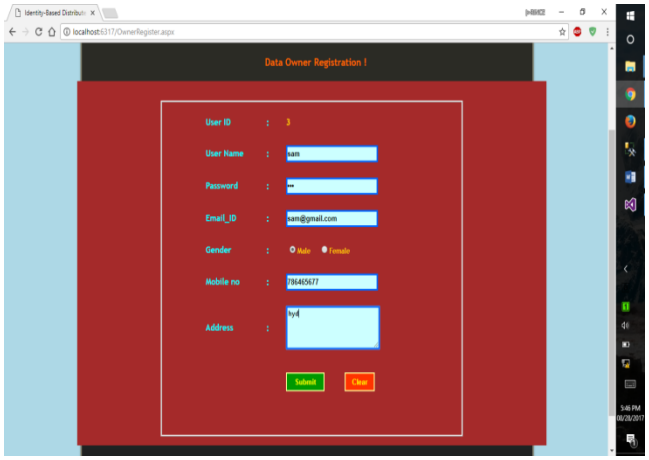
1) Security Mediated Cryptosystem: Mediated cryptography was first acquainted as a strategy with permit quick denial of open keys. The fundamental thought of interceded cryptography is to utilize an on-line middle person for each exchange. This on-line arbiter is alluded to a SEM (Security Mediator) since it gives a control of security abilities. On the off chance that the SEM does not participate then no exchanges with the general population key are conceivable any more. As of late, a trait based rendition of SEM was proposed. The thought of SEM cryptography was further modified as security interceded certificateless (SMC) cryptography. In a SMC framework, a client has a mystery key, open key and a personality. In the marking or decoding calculation, it requires the mystery key and the SEM together. In the mark verification or encryption calculation, it requires the client open key and the comparing character. Since the SEM is controlled by an expert which is utilized to deal with client renouncement, the specialist declines to give any collaboration to any disavowed client. In this way, disavowed clients can't produce signature or unscramble ciphertext. Note that SMC is not quite the same as our idea. The primary motivation behind SMC is to take care of the renouncement issue. Along these lines, the SME is controlled by the specialist. As it were, the specialist should be online for each mark marking and ciphertext decoding. The client isn't unknown in SMC. While in our framework, the security gadget is controlled by the client. Namelessness is additionally saved.

2) Key-Insulated Cryptosystem: The worldview of key protected cryptography was presented. The general thought of key-protected security was to store long haul enters in a physically-secure yet computationally-constrained gadget. Here and now mystery keys are kept by clients on some place cryptographic calculations occur. Toward the start of each day and age, the client gets an incomplete mystery key from the gadget. By joining this incomplete mystery key with the mystery key for the past period, the client recharges the

mystery key for the present day and age. Not the same as our idea, key-protected cryptosystem requires all clients to refresh their keys in each day and age. The key refresh process requires the security gadget. Once the key has been refreshed, the marking or decoding calculation does not require the gadget any longer inside a similar day and age. While our idea requires the security gadget each time the client tries to get to the framework. Moreover, there is no key refreshing required in our framework.

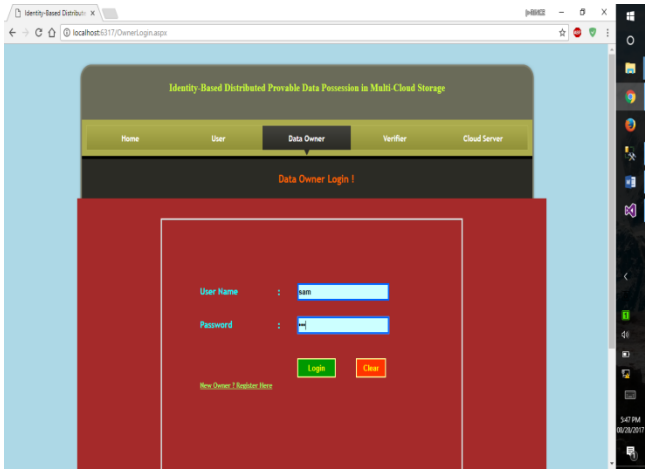
IV. IMPLEMENTATION & RESULTS

Below are some of the results of the project which demonstrates step by step process of entire application.



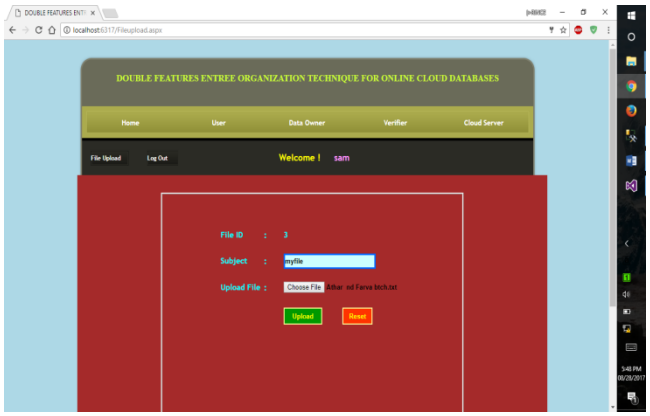
Output Screenshot 1: Registration page

In this page user can register to create an account by providing general information like username, password, email address and phone number to register. Once registration is completed, user can sign in the application.



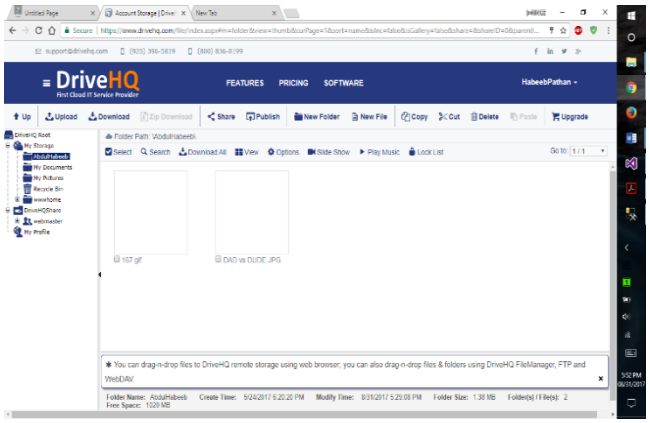
Output Screenshot 2: User Login page

Data Owner login page provides users to login in to the application and access it. User login page requires basic information to login like username, password. If the user credentials are correct, then users are authenticated.



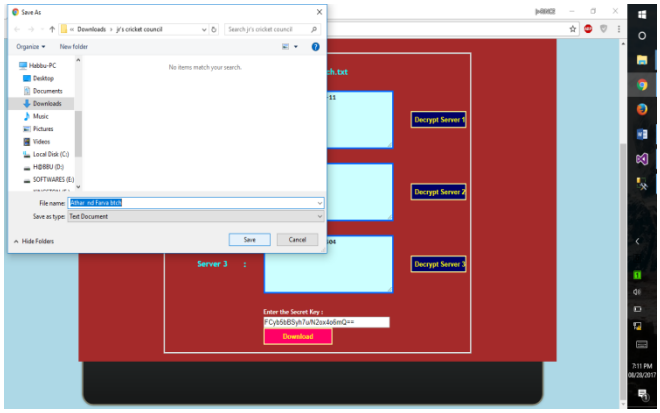
Output Screenshot 3: File upload page

After successful login in to the cloud server, file upload page is displayed to upload the file data in to the cloud server.



Output Screenshot 4: File upload in DriveHQ

the user will receive the uploaded content in cloud server.



Output Screenshot 5: file download

Here user can download their files by merging it. The download link will be provided after secure authentication in this page.

V. CONCLUSION

In this paper we propose a novel security algorithm called as 2FA with a pair of secret key and a light weight device in combination. Implementation of two factor authentication provides application security to

the next level. Basically, our proposed system works after the user is authenticated I.e. first user needs to provide his/her credentials which is a set of username and password for login in to the application. After successful login the next authentication process is called two factor authentications or second step verification. In this a user will receive a secret key on his/her device which is registered with the server. If user enters the correct secret key which they receive then they can access the entire application at that time.

VI. REFERENCES

[1]. Y. Dodis and A. Yampolskiy, proposed a paper "A verifiable random function with short proofs and keys," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3386, S. Vaudenay, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 416-431.

[2]. X. Huang et al., proposed a paper "Cost-effective authentic and anonymous data sharing with forward security," IEEE Trans. Compute., vol. 64, no. 4, pp. 971-983, Apr. 2015.

[3]. F. Xhafa, J. Wang, X. Chen, J. K. Liu, J. Li, and P. Krause, proposed a paper "An efficient PHR service system supporting fuzzy keyword search and fine-grained access control," Soft Compute., vol. 18, no. 9, pp. 1795-1802, 2014.

[4]. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, proposed a paper "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption," IEEE Trans.