International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN: 2456-172X | Vol. 2, No. 1, March - May, 2017 | Pages 111-118

# DESIGN OF SECURE AUTHENTICATED KEY MANAGEMENT PROTOCOL FOR CLOUD COMPUTING ENVIRONMENTS

R. Vinoth[1], R.Vidhya[2], V.Sabaresan[3]

*Assistant Professor[1, 2, 3], Department Of Information Technology[1, 2, 3],*
*Agni College of Technology[1, 2, 3], Chennai-600130[1, 2, 3], Tamil Nadu[1, 2, 3], India[1, 2, 3],*
*vinoth.it@act.edu.in[1], vidhya.it@act.edu.in[2], sabaresan.it@act.edu.in[3]*

## ABSTRACT

With the improvement of disseminated registering advancement to the extent trustworthiness and capability, incalculable organizations have moved to the cloud arrange. To worthwhile access to the organizations and guarantee the security of correspondence in the open framework, three-factor Mutual Authentication and Key Agreement shows for multi-server structures increment wide thought. In any case, most of the present three-factor MAKA shows don't give a formal security affirmation achieving various attacks on the related shows, or they have high estimation and correspondence costs. In addition, most of the three-factor MAKA shows haven't a dynamic denial segment, which prompts malicious customers cannot be speedily disavowed. To address these detriments, we propose a provable one of a kind revocable three-factor MAKA show that achieves the customer dynamic organization using Schnorr marks and gives a formal security proof in the subjective prophet. Security assessment exhibits that our show can fulfill various needs in the multi-server circumstances. Execution assessment demonstrates that the proposed arrangement is fitting for enrolling resource obliged smart contraptions. The full type of the reenactment execution shows the likelihood of the show.

## 1 INTRODUCTION

In the progressing decade, dispersed processing development has been completely advanced. It cannot simply improve organization capability yet moreover decrease costs. A regularly expanding number of associations are putting their organizations on the cloud arrange for development, the administrators and upkeep. This not simply decreases the area upkeep inconvenience for these undertakings, yet what's more gives bound together security and action the officials for all organizations on the untouchable cloud arrange.Yet pariah cloud stages have even more prevailing developments and continuously standard specific points of

interest to ensure that the servers continue running in a reasonably secure condition, customers and servers grant in the open framework. Along these lines, confirmation and key comprehension are essential for the correspondence security. The use of regular affirmation and key understanding shows not simply shield aggressors from abusing server resources, yet also foresee malicious aggressors acting like the server to get the customer's information.

**A EXISTING SYSTEM**

In any case, a large portion of the multiple servers don't give formal security evidence bringing about different assaults on the related conventions. By transferring the data there has some data loss. There has some third party access**.**

**EXISTING TECHNIQUE**

- Central server methods

**TECHNIQUE DEFINITION**

The computer itself may control all the peripherals directly (if they are physically connected to the central computer), or they may be attached via a terminal server. Alternatively, if the terminals have the capability, they may be able to connect to the central computer over the network.

**DRAWBACKS:-**

- Cannot guarantee the user’s privacy.
- High delay.

**B PROPOSED SYSTEM**

We proposed a Mutual Authentication and Key Agreement plot for multi-server conditions. Be that as it may, in their convention RC shares framework private key with all servers. This will provide the data transfer with high security and no data loss.

**PROPOSED TECHNIQUE**

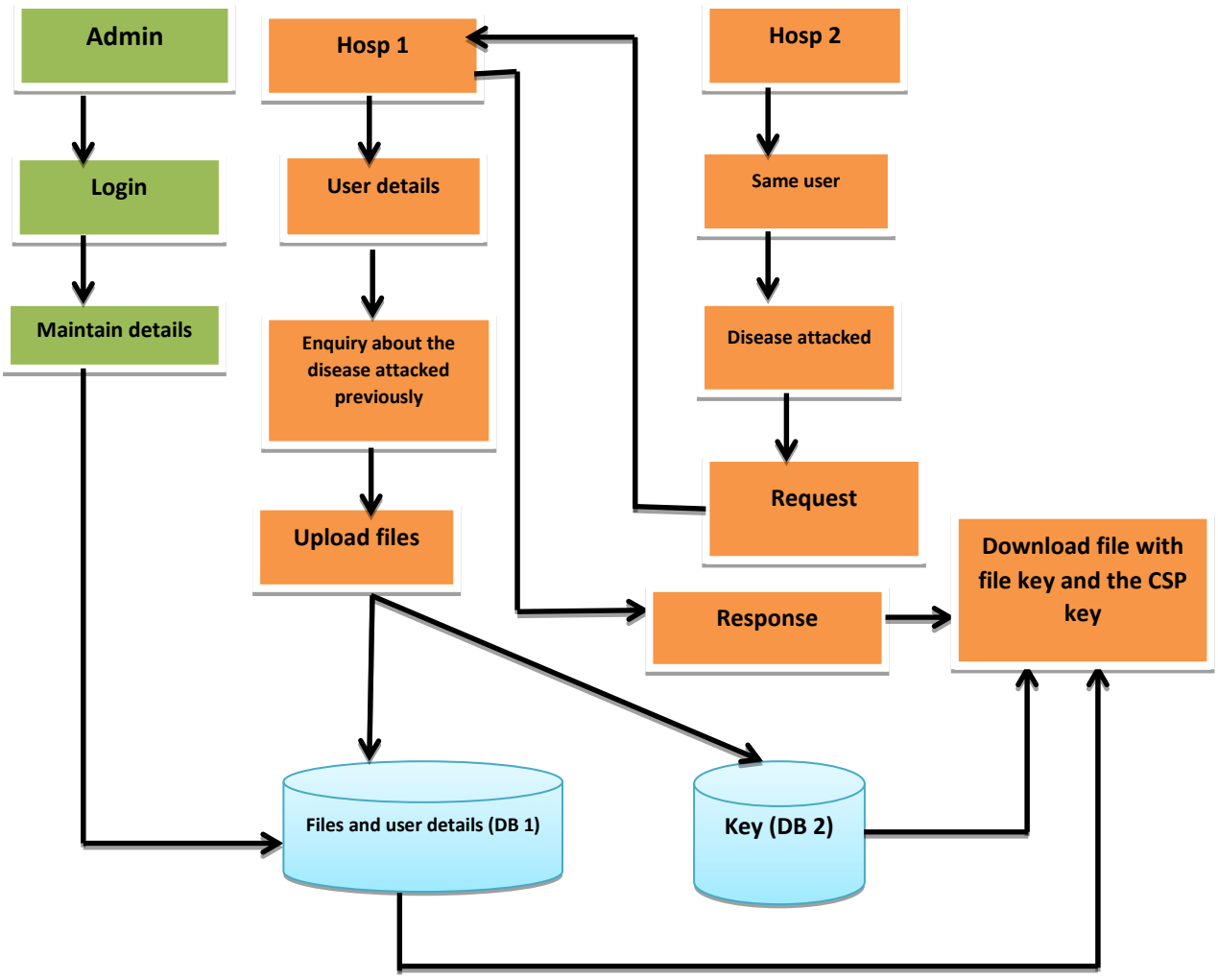
- MAKA

**TECHNIQUE DEFINITION**

Our plan accomplishes the client's dynamic administration. In our convention, clients can be powerfully denied to immediately keep assaults from malevolent clients.Without a dynamic renouncement Component, RC can'trebuffnoxious clients in a convenient way.

**ADVANTAGES**

- This will provide high security.
- Has no data loss.

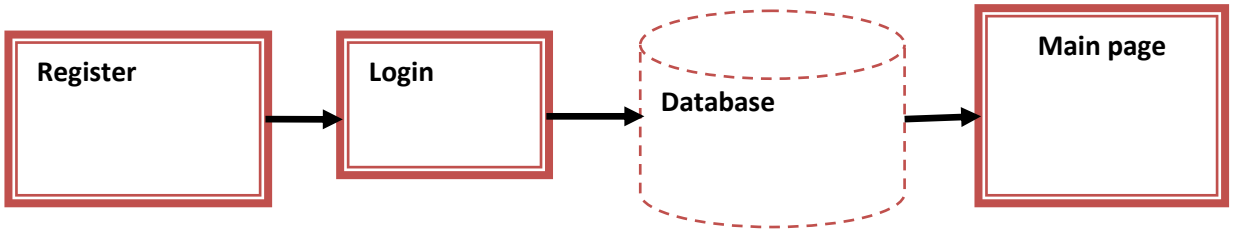



## II IMPLEMENTATION

### 1.USER INTERFACE DESIGN

This is the first module of our project. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page

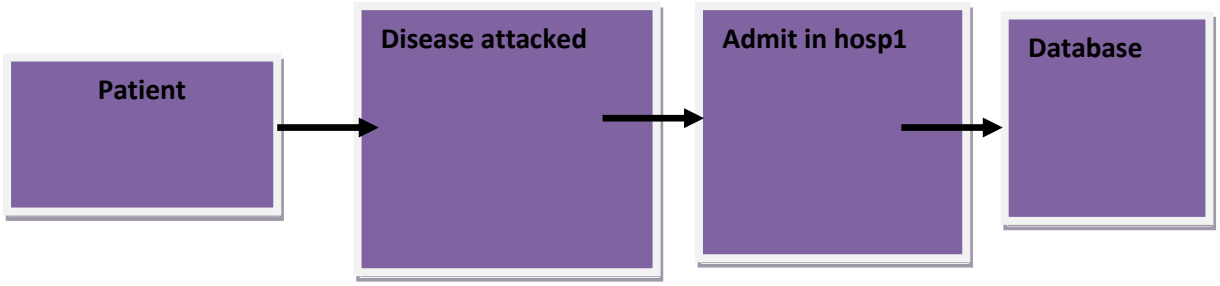
we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.




## 2. PATIENT GETTING ADMITTED IN HOSPITAL 1

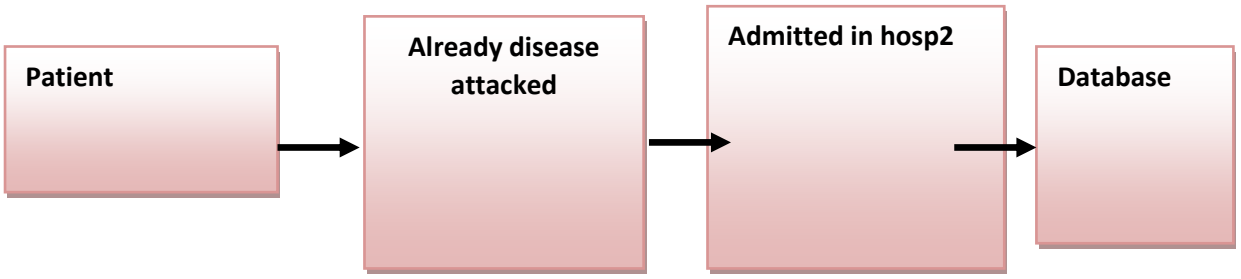
In this module, the user will be getting admitted in the hospital 1 due to some disease problem. After that the user information

regarding the treatment done for that disease and the tablets given everything will be stored in the database.



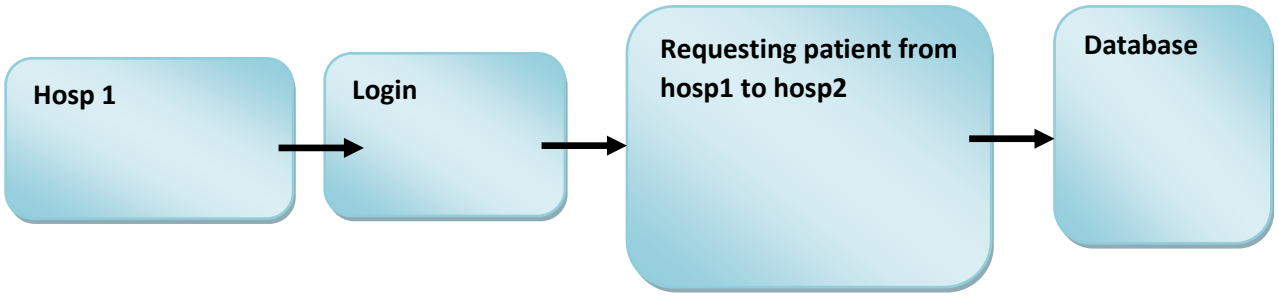

## 3. ALREADY DISEASE ATTACKED

In this module, the doctor will be asking the patient whether the disease is previously attack or not. If attacked, the doctor will be asking in what hospital you got admitted with this disease.



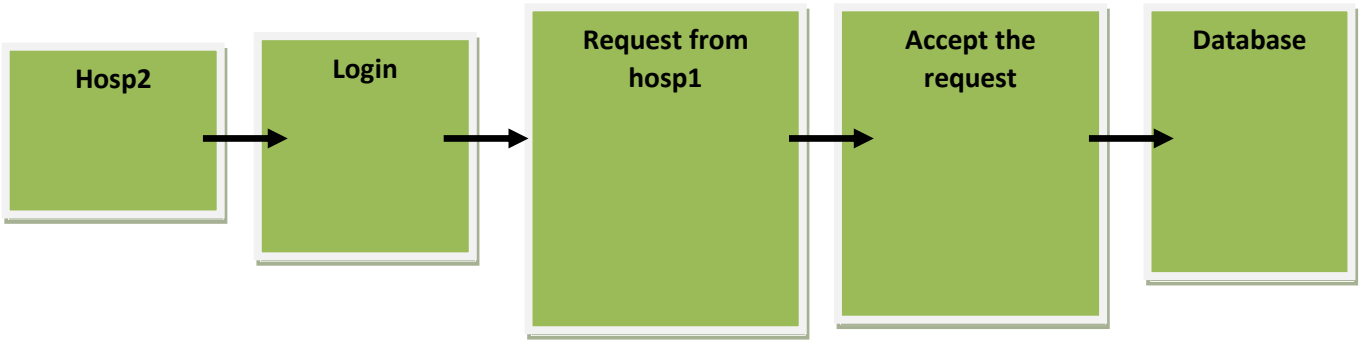
### 4. REQUEST PATIENT DATA FROM HOSP1 TO HOSP2

In this module, after knowing that the patient has admitted previously in hospital 1 the doctor will be requesting the patient treatment data and the tablets given from the hospital 2.



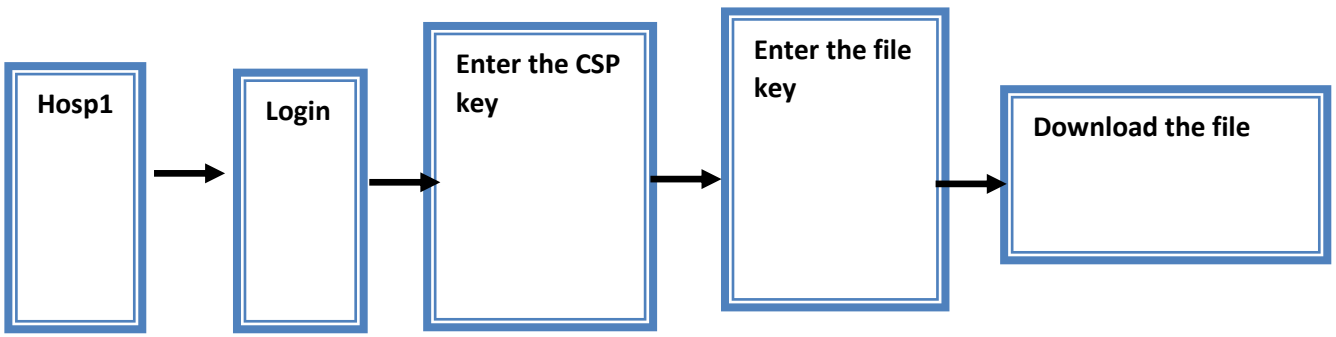

### 5. RESPONSE FROM HOSP2

In this module, after requesting the patient data from hospital 1, the hospital 2 will be accepting the request from the hospital 1 to know the treatment given to the patient.



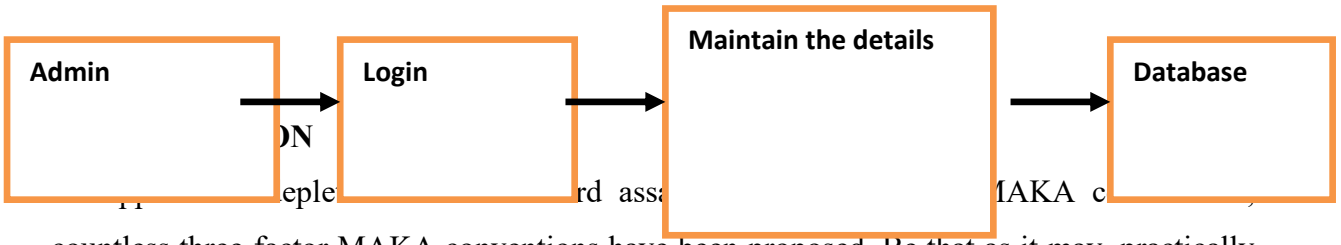

### 6. DOWNLOAD THE FILE USING THE KEYS

In this module, the doctor from the hospital 1 will be able to download the file using file key and the csp key provided to them and then the treatment will be started for the patient.




### 7. ADMIN MAINTAINING THE FILE

In this module, the admin will be maintaining the database the patient details and the hospital details.




**ON**

countless three-factor MAKA conventions have been proposed. Be that as it may, practically all threefactor MAKA conventions don't give formal verifications and dynamic client the executive's instrument. So as to accomplish increasingly adaptable client the board and higher security, this paper proposes another three-factor MAKA convention that underpins dynamic denial and gives formal verification. The security demonstrates that our convention accomplishes the security properties of necessities from multi-server conditions. Then again, through the extensive investigation of execution, our convention doesn't forfeit effectiveness while improving the capacity. Unexpectedly, the proposed convention has incredible preferences as far as the absolute calculation time.

## IV FUTURE ENHANCEMENT

## FUTURE CONCEPT

Our future works include a real implementation for the secure data sharing scheme.

**FUTURE TECHNIQUE**

- Identity-based Encryption

**TECHNIQUE DEFINITION**

ID-based encryption, or identity-based encryption (IBE), is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). This means that a sender who has access to the public parameters of the system can encrypt a message using e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its decryption key from a central authority, which needs to be trusted as it generates secret keys for every user.

**REFERENCE:**

[1] L. Lamport, "Password authentication with insecure communication," Communications of The ACM, vol. 24, no. 11, pp. 770–772, 1981.

[2] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 8, pp. 1390–1397, 2011.

[3] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Robust multifactor authentication for fragile communications," IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 6, pp. 568– 581, 2014.

[4] D. He, S. Zeadally, N. Kumar, and J. Lee, "Anonymous authentication for wireless body area networks with provable security," IEEE Systems Journal, pp. 1–12, 2016.

[5] L. Li, L. Lin, and M. Hwang, "A remote password authentication scheme for multiserver architecture using neural networks," IEEE Transactions on Neural Networks, vol. 12, no. 6, pp. 1498–1504, 2001.

[6] W. Juang, "Efficient multi-server password authenticated key agreement using smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 251–255, 2004.

[7] C. C. Chang and J. S. Lee, "An efficient and secure multi-server password authentication scheme using smart cards," in International Conference on Cyberworlds, 2004, pp. 417–422.

[8] J.-L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table," Computers & Security, vol. 27, no. 3C4, pp. 115–121, 2008.

[9] W. Tsaur, J. Li, and W. Lee, "An efficient and secure multi-server authentication scheme with key agreement," Journal of Systems and Software, vol. 85, no. 4, pp. 876–882, 2012.

[10] Y. Liao and C. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients," Future Generation Computer Systems, vol. 29, no. 3, pp. 886–900, 2013.