International Journal of Scientific Research and Engineering Development-– Volume 3 Issues 1 Jan- Feb 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

DESIGN OF SECURE AUTHENTICATED KEY MANAGEMENT PROTOCOL BETWEEN ORGANIZATIONS

S.Gayathri*, M.Sangeetha**,S. Priyanka***

*(Assistant Professor, Computer Science And Engineering, Jeppiaar SRR Engineering College, Padur, Chennai)

** (Computer Science And Engineering, Jeppiaar SRR Engineering College, Padur, Chennai
Email:msangeetha1502@gmail.com)

*** (Computer Science And Engineering, Jeppiaar SRR Engineering College, Padur, Chennai
Email:priyankasakthivelan@gmail.com@gmail.com)

----------**********----------

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.

Keywords —MAKA,CSP,AES.

----------**********----------

I. 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.

II. RELATED WORKS

An efficient multi-server password authenticated key agreement scheme using smart cards with access control, Chin-Chen Chang ; Jui-Yi Kuo, (2005) [1].Due to the fast development of science and techniques, folks will remotely access computers over the networks. Thus, user authentication and key agreement become additional and additional vital to make sure the lawfulness of the user and also the security of later communications, severally. as a result of the amount of servers providing the facilities for the user is typically quite one, the thought of multi-server protocols is introduced. On the net, every server typically provides numerous services, and every service provided by the server might not be accessed by the user. Hence, access management is needed within the multi-service setting. In 2004, Juang planned a multi-server authentication theme with key agreement. However, access management isn't taken into consideration in Juang's planned theme, therefore we have a tendency to propose associate economical multi-server secret genuine key agreement theme with access management during this article.

On the security of ID-based password authentication scheme using smart cards and fingerprints,Chu-Hsing Lin ; Tri-Show Lin ; Hsiu-Hsia Lin ; (2005) [2].In 2003, Kim, Lee and Yoo projected an ID-based password authenticationscheme for log-on to a distant server mistreatment revolving credit, parole and fingerprint. during this paper, we tend to show that the KLY protocol is liable to an energetic resister United Nations agency will extract some data embedded within the revolving credit by mistreatment existing good cards attack ways. By obtaining the knowledge and eavesdropping the previous login messages of a legal user, Associate in Nursing aggressor with none parole or fingerprint will with success forge the legal user to get services from the system. during this case, the protocol isn't adequate for systems with high level security necessities.

Efficient and Secure Remote Authenticated Key Agreement Scheme for Multi-server Using Mobile Equipment, Jun Ho Lee; Dong Hoon Lee (2008) [3]. This paper presents a cost-effective and secure documented key agreement theme between remote users and multi-servers. The theme is employed for mutual authentication and session key agreement between mobile devices and application servers, notably mobile phones equipped with IC (Integrated Circuit) chips sort of a wise card or a USIM (Universal Subscriber Identity Module) card for 3G. and additionally the theme could be a heap of merely enforced to mobile devices and efficiently utilized in mobile setting because of victimization light-weight operation functions like commonplace, hash and XOR.

A Reliable Dynamic User-Remote Password Authentication Scheme over Insecure Network Publisher, Zhen-Yu Wu ; Dai-Lun Chiang; Yu-Fang Chung ; Tzer-Shyong Chen. (2012) [4].Protocols of user authentication are ready to make sure the security of knowledge transmission and users' communication over insecure networks. Among numerous authenticated mechanisms run presently, the password-based user authentication, owing to its potency, is that the most generally used in several areas, like laptop networks, wireless networks, remote login, operation systems, and direction systems. when countersign is endowed with the property of straightforward and human unforgettable, that causes such AN attack of brute force, as an example, the previous works typically suffer off-line countersign idea attack. Therefore, AN meliorative password-based authentication theme is planned during this paper, achieving to resist off-line countersign idea attacks, replay attacks, on-line countersign idea attacks, and ID-theft attacks. In lightweight of security, the planned theme is supplied with smart utility, even over insecure network.

Robust Multi-Factor Authentication for Fragile Communications, Xinyi Huang ; Yang Xiang ; Elisa Bertino;(2014) [5]. In large-scale systems, user authentication typically wants the help from a far off central authentication server via networks. The authentication service but may be slow or untouchable thanks to natural disasters or numerous cyber-attacks on communication channels. This has raised serious considerations in systems which require strong authentication in emergency things. The contribution of this paper is two-fold. in a very slow affiliation scenario, we tend to gift a secure generic multi-factor authentication protocol to hurry up the complete authentication method. Compared with another generic protocol within the literature, the new proposal provides identical operate with important enhancements in computation and communication. Another authentication mechanism, that we tend to name complete authentication, will demonstrate users once the affiliation to the central server is down. we tend to investigate many problems in complete authentication Associate in Nursingd show means toa way to add it on multi-factor authentication protocols in an economical and generic way.

III. LIMITATIONS OF EXISTING SYSTEM

- There has been a large portion of the multiple servers donot give formal security evidence bringing about different assaults on the related conventions.
- There has some third party access and so there cannot guarantee the user's privacy.
- There is a high delay and also has some loss of data while transferring.
- As the exsisting system uses center server database there is high loss of data and also have security related problems.

IV. PROPOSED SYSTEM

The technique of Mutual Authentication and Key Agreement(MAKA) is used which provides the secured and allows the user to authenticate for the data to be shared between two hospitals. By using this technique, it ensures increase in reliability and security. Here, when the hospital needs the patients treatment details then that hospital has to forward the request to the hospital where that patient got admitted previously. By using the unique id(Aadhar number) the details of the previous hospital name, doctor name, etc., will be given to the required hospital. Then the response will be forwarded to the requested hospital for further treatment.

An increasingly proficient Shared Authentication and Key Agreement plot for multi-server conditions is used. 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't rebuff noxious clients in a convenient way.

Thus our project has critical points of interest as far as customer figuring time and complete cost time. This enables our convention to be conveyed on savvy gadgets that have constrained processing power.It alsoguarantee the user's privacy. There is no delay and also more secure.

V. SYSTEM DESIGN

The proposed architectural model of this project is as shown in the figure 2.

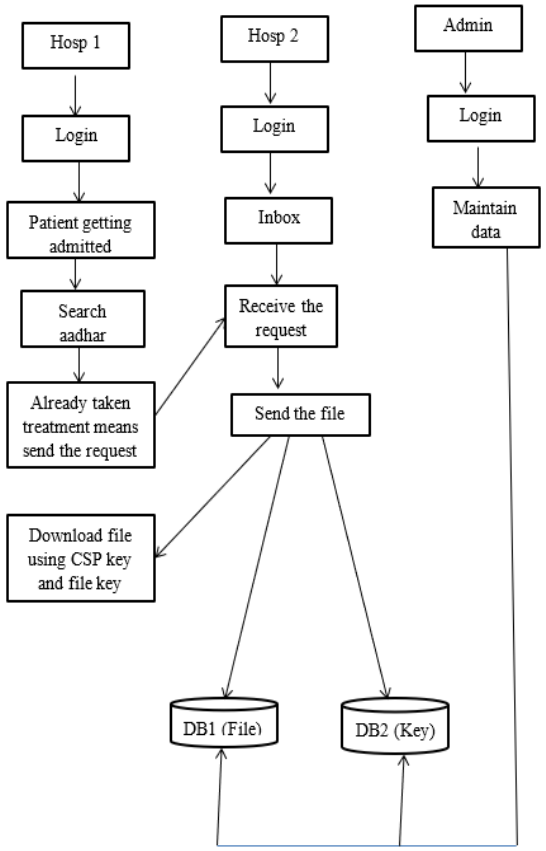

Fig 1: Overall Architecture

MODULES

- Registration of two hospitals
- Patient Registration
- Requesting file
- Response from DataBase
- Downloading the file using the keys
- Admin maintenance

1. Registration of two hospitals

The vital role for the user is to maneuver login window to user window. This module has created for the protection purpose. during this login page we've to enter login user id and word. it'll check username and word is match or not (valid user id and valid password). If we have a tendency to enter any invalid username or word we have a tendency to can't enter into login window to user window it'll shows error message. This has got to be in hot water every and each hospial furthermore as admin. then the CSP key are generated and it's to be noted down for preventing the dettails from unauthorized user getting in the login window to user window. it'll give an honest security for our project. thus server contain user id and word server conjointly check the authentication of the user. It well improves the protection and preventing from unauthorized user enters into the network. In our project we have a tendency to area unit victimisation JSP for making style. Here we have a tendency to validate the login user and server authentication.

2. Patient Registration

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 disease and the patients unique id (aadhar number) will be stored in the database. And the doctor will be asking the patient whether the disease is previously
attacked or not. If attacked, the doctor enquires the patient about the previously attacked diseases and the hospital name that he got treatment previously.

3. Requesting file

The patients unique id(aadhar number)is used to findhospital name,doctorname,phonenumber,etc., that they got treatment previously.After that the request will be sent to that hospital for getting the patients treatment details.So requesting file is done successfully using patients unique id.

4. Response from DataBase

The request sent by the hospital for getting details will be received in the notification. After receiving the notification the hospital needs to attach required file. Then the hospital needs to upload the exact patient treatment details from the database and unique file key will be generated for that particular file. Then the file will be uploaded successfully.

5. Downloading the file using the keys

The hospital which requested the patients treatment details needs to download the file using the csp key and the unique file key. The filedownload will be done by entiring the exact csp key
and the file's key. If both the keys gets matched the the file will be downloaded successfully. After that the downloaded file will be used for further treatment. If the keys are not matched the file will not be downloaded.

6. Admin maintanance

The admin maintain the details like how request sent to the hospitals, how the responses are sent from the hospitals as well as how many requests and responses are sent, what are all the files been uploaded, what are all the files been downloaded for the patients treatment. The main purpose of the admin is to maintain the database regularly.

DATA FLOW DIAGRAM

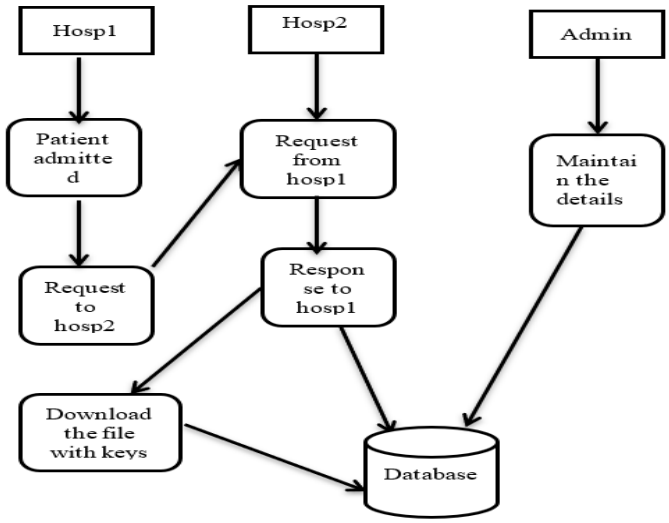

Fig. : 3 Data flow diagram

ALGORITHM OR MOTHODOLOGY:

AES

Data Integration is that the mixture of technical and business processes wont to combine data from disparate sources into meaningful and valuable information. The process of data Integration is about taking data from many disparate sources (such as files, various databases, mainframes etc.,) and mixing that data to provide a unified view of the data for business intelligence. Data integration is required when a business decides to implement a replacement application and migrate its data from the legacy systems into the new application. It becomes even critically important in cases of company mergers where two companies merge and that they got to consolidate their applications. One of the most commonly known uses of data integration is building a data warehouse for an enterprise which enables a business to have a unified view of their data for analysis and business intelligence needs.

VI.RESULTS AND DISCUSSION

Mutual Authentication and Key Agreement (MAKA) is used. The fig:4 shows the patients unique id(aadhar number)is used to find the hospital name, doctor name, phone number, etc., that they got treatment previously.

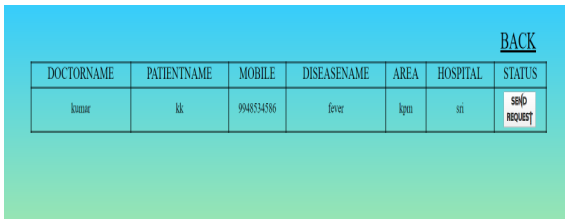

Fig.: 4 Finding hospital name using unique id

After that the request will be sent to that hospital for getting the patients treatment details. So requesting file is done successfully using patients unique id. This is shown in fig:5

Fig.: 5 Sending request

The hospital which requested the patients treatment details needs to download the file using the CSP key and the unique file key. The file download will be done by entiring the exact CSP key and the file's key. This is shown in fig:6

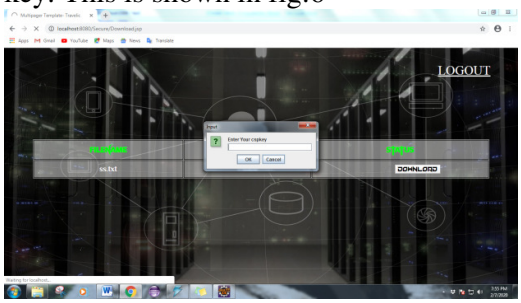

Fig.: 6 Matching with the keys

If both the keys gets matched the file will be downloaded successfully.Afterthat the downloaded file will be used for further treatment. If the keys are not matched the file will not be downloaded. This is shown in fig:7

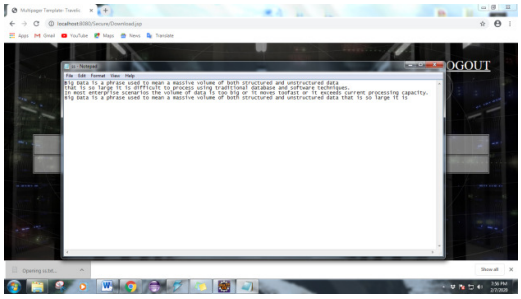

Fig.: 7 Downloading the file

VII. CONCLUSION

On these research paintings we've proposed a project to oppose the depletion of secret word assault on the two-factor MAKA conventions, countless three-factor MAKA conventions have been proposed. Be that as it may, practically all three factor 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. Thenagain, 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.

VIII. REFERENCE

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

[2] 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.

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

[4] H. Kim, S. Lee, and K. Yoo, "Id-based password authentication scheme using smart cards and fingerprints," Operating Systems Review, vol. 37, no. 4, pp. 32–41, 2003.

[5] 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.

[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]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.

[8] 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.

[9] 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.

[10] 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.

[11] D. Wang and P. Wang, Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards. Springer International Publishing, 2015.

[12] 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.

