International Journal of Research in Engineering, Science and Management
Volume-3, Issue-3, March-2020
www.ijresm.com | ISSN (Online): 2581-5792

Design of Secure Authenticated Key Management Protocol for Cloud Computing Environment

K. Ramya[1], S. Swathi Khanna[2], M. Vidya[3], M. Helda Mercy[4]
[1,2,3]*B.Tech. Student, Department of Information Technology, Panimalar Engineering College, Chennai, India*
[4]*Professor, Department of Information Technology, Panimalar Engineering College, Chennai, India*

***Abstract*: With the advanced 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, three factor MAKA (Mutual Authentication and Key Agreement) protocol is used. Firstly, user interface is designed to allow the authenticated user to access the service. While accessing the patient medical records, there are many security issues raises such as extraordinary research accomplishments on secret key security, passwords are as yet broken because of client's imprudent practices. We propose three factor MAKA protocol to solve the issues and to improve advantage of cloud storage and Privacy of data. It provides the data transfer with high security and reduces data loss.**

***Keywords*: Key management protocol, Three factor Mutual Authentication and Key Agreement, Cloud computing, Password, Security.**

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 put 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 is 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. Online administrations have developed, in which secret phrase confirmation is the most broadly utilized verification technique, for it is accessible requiring little to no effort and simple to send Consequently, secret phrase security consistently draws in incredible interest from the scholarly community also, industry. In spite of extraordinary research accomplishments on secret key security, passwords are as yet broken since clients' imprudent practices. For example, numerous clients frequently select frail passwords; they will in general reuse same passwords in various frameworks. They normally set their passwords utilizing recognizable jargon for its benefit to recall. Moreover, framework issues may cause secret word settles. It is very hard to get passwords from high security frameworks. On the one hand, taking verification information tables (containing usernames and passwords) in high security frameworks is troublesome.

2. Literature survey

The first survey of detecting site visitors from social media as [1] Zhen-Yu Wu dialect, et. al., presents the survey paper A Reliable Dynamic User-Remote Password Authentication Scheme over Insecure Network Publisher at 2012. Protocols of user authentication square measure able to make sure the security of information transmission and users' communication over insecure networks. Among varied documented 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. as it is blessed with the property of straightforward and human unforgettable, that causes such associate degree attack of brute force, for instance, the previous works typically suffer off-line password shot attack. Therefore, associate degree meliorative password-based authentication theme is projected during this paper, achieving to resist off-line password shot attacks, replay attacks, on-line password shot attacks, and ID-theft attacks. In lightweight of security, the projected theme is given sensible utility, even over insecure network.

[2] Xinyi Huang, et. al., presents the survey paper of Robust Multi-Factor Authentication for Fragile Communications at 2014. In large-scale systems, user authentication sometimes needs the assistance from the central authentication server via networks. The authentication service might be down or

unavailable to natural disasters or various cyber-attacks on communication channels. This has raised serious considerations in systems which require sturdy authentication in emergency things. The contribution of this paper is two-fold. During a slow affiliation scenario, we have a tendency 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 an equivalent perform with vital enhancements in computation and communication. Another authentication mechanism, that we have a tendency to name complete authentication, will manifest users once the affiliation to the central server is down. We have a tendency to investigate many problems in complete authentication and show how to add it on multi-factor authentication protocols in an economical and generic way.

[3] Chin-Chen Chang, et. al., presents the survey paper of an efficient multi-server password authenticated key agreement scheme using smart cards with access control. Due to the speedy development of science and techniques, users will remotely access computers over the networks. Thus, user authentication and key agreement become additional and additional vital to confirm 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 sometimes over one, the idea of multi-server protocols is introduced. On the web, every server sometimes provides varied services, and every service provided by the server might not be accessed by the user. Hence, access management is needed within the multi-service atmosphere. In 2004, Juang planned a multi-server authentication scheme with key agreement. However, access management isn't taken under consideration in Juang's planned scheme, therefore we have a tendency to propose. An economical multi-server password authentication key agreement theme with access management during this article.

[4] Chu-Hsing Lin, et al., presents the survey paper of On the security of ID-based password authentication scheme using smart cards and fingerprints at 2005. This paper proposes the algorithm of two id based password authentication schemes where there is no need of passwords or verification tables such as smart card and fingerprint. With this schemes, user can easily change their passwords. The proposed nonce based authentication scheme can withstand the occurrence of message replay attacks for a network without synchronization clocks. These schemes require each user's knowledge, possession and biometrics for each user authentication and this feature makes our scheme more reliable.

[5] Jun Ho Lee, et al., presents the survey paper of Efficient and Secure Remote Authenticated Key Agreement Scheme for Multi-server Using Mobile Equipment. This paper proposes the algorithm of efficient secured authenticated key agreement scheme between remote users and multi servers. The mutual authentication and session key agreement scheme is used between mobile devices equipped with IC (Integrated Circuit) chips such as USIM (Universal Subscriber Identity Module) card for 3G or smart card and application server. On using light operation functions such as modular, hash and XOR, those scheme can be more easily implemented to mobile devices and used efficiently in mobile environment.

3. Methodology

For ensuring authentication among the hospitals, here we are using MAKA protocol which stands for Mutual Authentication and Key Agreement. This protocol approaches the technique in which various hospital in the cloud has been mutually authenticated through CSP key where it is a uniquely generated key form for each new user and the key agreement has been done through exchanging the file keys by request and response form. Here we are using two databases, one for storing files and user details and other for storing keys. Here we are using two keys namely CSP key and file key. These keys are which is mainly using for authentication process. In this condition patient is getting admitted in one hospital due to some reasons after certain period of time the same patient is getting hospital in another hospital. To know the information about the treatment details of the patient. The various hospitals in the cloud is get communicate with each other by sending request about the particular patient, the response has been sent to the requested patient details. Firstly, in hospital1 the user details have been get collected from the user like name, age, weight, height etc.

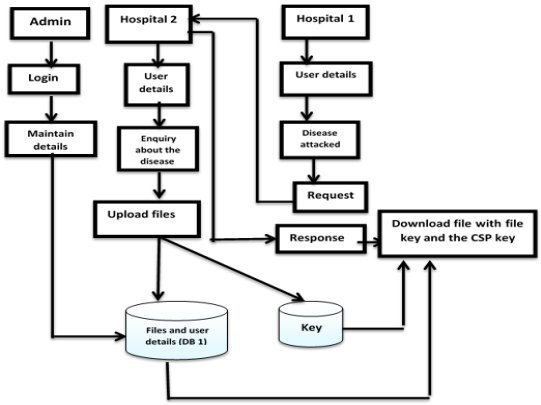

Fig. 1. System architecture

Then hospital-1 is enquiring about the previously attacked disease for the patient then upload the files in the databases. If same user there in another hospital that is hospital-2 if some disease is attacked then they will verify whether the patient is attacked by the same disease previously if so they will send the request to the particular hospital, by receiving the response from the another hospital that is file to download it there will be a need of two keys one key is CSP key and another one is file key. By entering correct keys, the file will be get downloaded automatically. The admin will get login and maintain those hospital details in the Cloud. The modules contain in the project are:

A. *Authentication*

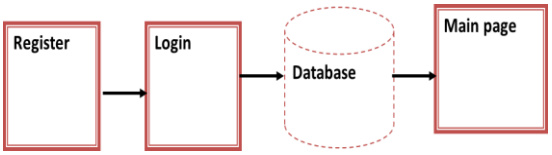

Fig. 2. Authentication

In this module, the vital role of the user is to register and move from login window to user window. This module has created for the protection purpose and during this login page user have to enter login user id and password. Authentication process takes place, if it tends to be an invalid data it shows an error page to prevent from unauthorized user. If the entered user login data is valid then it moves to the next page. Thus server contain user id and password 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 tend to use victimization JSP for making style. Here we tend to validate the login user and server authentication.

B. *Patient database*

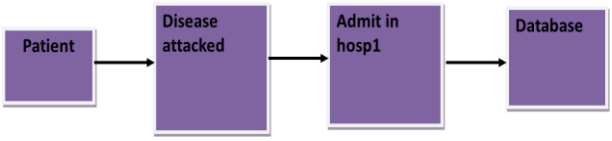

Fig. 3. Patient details

In this module, the patient is get admitted in the hospital. Information regarding the patient details like emergency contacts, address, contact number are get collected and stored in database.

C. *Information retrieval and transmission*

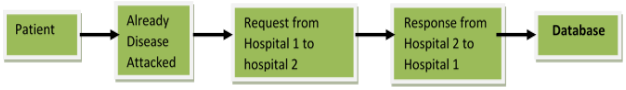

Fig. 4. Information retrieval and transmission

In this module, the doctor will be getting the information about the previously attacked disease and where the treatment has been undergone and this information are stored in database. If, the doctor gets to know about the previously attacked disease and where the treatment has been undergone. The request will be sent to the respective hospital regarding information about the patient details and disease attacked. After the request sent to the respective hospital. The hospital 2 get to know about the request, if any so the patient details and treatment undergone will be attached and sent to the hospital 1 as a response by accepting the request. Hospital 2 sends the file and file key to the hospital 1.

D. *Key exchange module*

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.

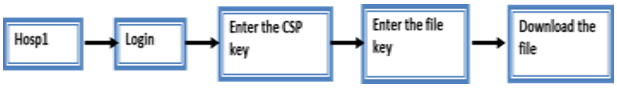

Fig. 5. Key exchange module

E. *Admin module*

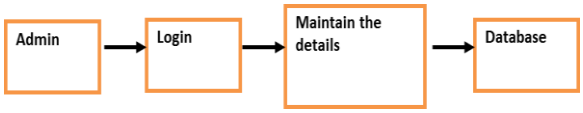

Fig. 6. Admin module

In this module, the admin will maintain the details in the database and this details includes hospital details, patient details and uploaded file details.

4. Conclusion

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. 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.

References

[1] Zhen-Yu Wu; Dai-Lun Chiang; Yu-Fang Chung; Tzer-Shyong Che, "A Reliable Dynamic User-Remote Password Authentication Scheme over Insecure Network Publisher",2012.
[2] Xinyi Huang; Yang Xiang; Elisa Bertino, Robust Multi-Factor Authentication for Fragile Communications",2014.
[3] Chin-Chen Chang; Jui-Yi Kuo; "An efficient multi-server password authenticated key agreement scheme using smart cards with access control", 2005.
[4] Chu-Hsing Lin; Tri-Show Lin; Hsiu-Hsia Lin; "On the security of ID-based password authentication scheme using smart cards and fingerprints", 2005.
[5] Jun Ho Lee; Dong Hoon Lee;" Efficient and Secure Remote Authenticated Key Agreement Scheme for Multi-Server Using Mobile Equipment", 2008.
[6] L. Lamport, "Password authentication with insecure communication," Communications of The ACM, vol. 24, no. 11, pp. 770–772, 1981.
[7] 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.
[8] 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.
[9] 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.

[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] 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.