Providing Security in Multiserver Authentication Scheme using Efficient Three Factor Encryption

Mohammad Majid Masroor, Kushagra Mishra, E. Sasikala

***Abstract:** For last couple of months, Using Two Factor Authentication was not so secure to protect the data inheriting from Multiserver Authentication. Providing Three Factor Authentication helped a lot in these fields to enhance the security while decrypting the encrypted files but failed in many aspects as there were no Multiserver Authentication was used. Here, the approach is used to provide security in Multiserver Platform Using Three Factor Encryption efficiently so as to remove 99.9% chances of failure in security from decryption of the files without going through Three Factor Security present at different Servers to verify at same time and providing permission to access. For the duration between Feb. 2019 and Jan 2020, There were millions of cases reporting loss of data even having two factor authentication, It happens in a way to get through the first factor on first server taking approval, and the packet can be dropped in-between to use that authentication to get through the second factor on second server to access the data. With the improvement of spread choosing development to the degree unfaltering quality and point of confinement and boundless affiliation have been set as parameters to improve. So, we have implemented these changes in our model to reduce the complexity by this effect providing more security using different layers and format to keep the file secure and going through 3-layer security and authentication before getting access.*

***Keywords:** Authentication, Factor, Multiserver. Two, Three*

I. INTRODUCTION

The advancing decade and the need for cloud computing technology has increased manifold. Cloud computing technologies not only increase service efficiency but also help in reducing cost. With the increasing demand of cloud computing technologies more companies are adapting it and putting their various services of maintenance and management on the cloud platform. With the availability of these services on a cloud the local server burden is also decreased and also a much more secure form of communication as well as data transfer medium is built as shown in Fig 1. Third party cloud environment are more secure as compared to other cloud environments. They provide user confidentiality and also ensure that the servers using Mutual Authentication Key Agreement (MAKA) protocols because they prevent attackers from misusing the server’s resources and prevent attackers from faking a server to extract important information. To provide a much more secure MAKA protocol various studies have being conducted after Lamport proposal of a password-based authentication protocol [1]. In the beginning various MAKA protocols[2],[3],[4] were designed. All these protocols were meant for a single server architecture. As the technological wild fire spread across the globe the users using various cloud services increased manifold. Since the protocol was meant for a single server architecture it became a difficult task for the user to remember different password for each server. To overcome these problems new and more advanced MAKA protocols [5],[6],[7],[8],[9],[10] were discovered. These enhanced protocols involved the usage of multi-server environment. These protocols were convenient to use after the application of appropriate management features..

Manuscript received on May 25, 2020.
Revised Manuscript received on June 29, 2020.
Manuscript published on July 30, 2020.
***** Correspondence Author

Mohammad Majid Masroor*, Computer Science & Engineering, SRM Institute of Science and Technology, Chennai, India. E-mail: majidmasroor@gmail.com

Kushagra Mishra, Computer Science & Engineering, SRM Institute of Science and Technology, Chennai, India. E-mail: kushagramishra999@gmail.com

E.Sasikala, Computer Science & Engineering, SRM Institute of Science and Technology, Chennai, India. sasikalaksr@gmail.com

II. RELATED WORKS

A. Security Layer Analysis

In 2001, Li et al[4] wrote this journal and proposed a much secure and reliable technique. They proposed the use of asymmetric cryptography to encrypt and decrypt the records. They proposed the use of Identity Based Encryption(IBE) algorithm. Asymmetric Cryptography is a type of cryptography that uses two different keys for encryption and decryption. In their proposed technique the public key was supposed to be the IP address of the destination computer and the private key is supposed to be generated at the receiver’s end by using a trusted PKG mechanism. Further in their study they proposed the use of three different servers to encrypt and decrypt the records and send the record to the correct recipient without compromising the integrity of the record. The use of three servers as shown in Figure 2.1 shows greater efficiency in encryption and decryption of the records as proposed in earlier two server system.

B. Encryption Analysis

In 2012 Zhen et al proposed A Reliable Dynamic User-Remote Password Authentication Scheme over Insecure Network Publisher. In his paper he discussed about conventions of client verification can guarantee the security of information transmission and clients' correspondence over unreliable systems.

Among different verified components run presently, the secret phrase based client validation, in light of its proficiency, is the most generally utilized in various territories, for example, PC systems, remote systems, remote login, activity frameworks, and database the board frameworks. [24],[25],[26], Indeed, even as secret word is enriched with the property of basic and human important, for which causes such an assault of animal power, for instance, the past works frequently endure disconnected secret word speculating assault. Along these lines, an ameliorative secret key based validation conspire is proposed in this paper, accomplishing to oppose disconnected secret phrase speculating assaults, replay assaults, on-line secret key speculating assaults, and ID-burglary assaults. Considering security, the proposed plan is given acceptable practicability, much over shaky system.

C. Authentication Analysis

In 2014 Xinyi et al proposed Robust Multi-Factor Authentication for Fragile Communications. In his paper he discussed colossal scale structures, customer approval regularly needs the assistance from a remote central affirmation server by methods for frameworks. The approval organization in any case could be moderate or blocked off on account of disastrous occasions or distinctive advanced attacks on correspondence channels. This brought veritable stresses up in structures which need solid affirmation in emergency conditions. The responsibility of paper is two-cover. In a moderate affiliation situation, we present an ensured nonexclusive multifaceted affirmation show to quicken the whole confirmation process. Differentiated and another regular show in the composition,new recommendation outfits a comparative limit with vital improvements in computation correspondence. Another approval instrument, which we name stay lone affirmation, can confirm customers when relationship with the central server is down. We analyze a couple of issues in stay lone approval and advise the most ideal approach to incorporate it multifaceted affirmation shows in a capable and nonexclusive way

D. Inference from the Survey

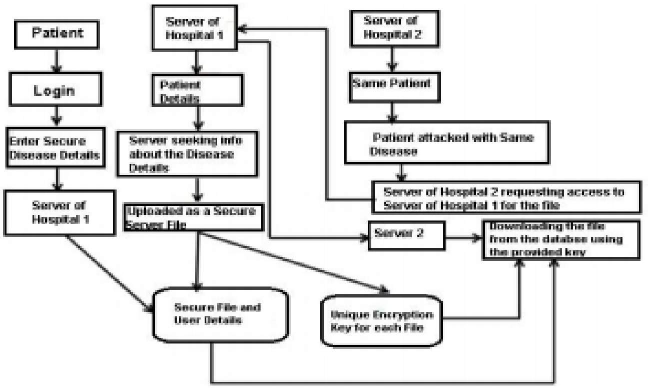
An implementation of MAKA Algorithm to increase the stability as well as security provided us the Extended Usage of OFB(Outback Feedback) or CTR(Counter) mode as well as Increased Symmetry of Cryptography by using Encryption and Decryption as high security measures which as a conclusion gave us the High Detection measures due to authorization through biometric and due to which we were able to achieve the results to secure Three Layer Authentication.

III. MAKA PROTOCOL USING THREE FACTOR AUTHENTICATION

Providing Security with Three Factor Authentication Model: While Providing all the details and part of procedure in this model, It also includes three factor Authentication within MAKA Protocol using the analysis and design of the security layer to provide the best results making the time complexity to be lowest and the security transformation to be the best.

A. User Interface Design

This is the very first step or it can be said the very first module of this proposed technique. In this module the user will interact with the system via a login. This is the first level and the most basic form of authentication. The user will be shown a login window where he will have to enter his unique login id and password. After he has entered his login ID and password the system with authenticate it. If the id or the password is invalid it will generate an error and will prevent the user from login in. This will help in preventing unauthorized access to the system. This will also grant our system immunity over illegal access from hackers. This login page is designed using JSP and here the validation of login and password is done by the server.


Patient
Login
Enter Secure Disease Details
Server of Hospital 1
Server of Hospital 1
Patient Details
Server seeking info about the Disease Details
Uploaded as a Secure Server File
Server of Hospital 2
Same Patient
Patient attacked with Same Disease
Server of Hospital 2 requesting access to Server of Hospital 1 for the file
Server 2
Downloading the file from the databse using the provided key
Secure File and User Details
Unique Encryption Key for each File

B. Dataset Collection

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 and 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

C. Data Processing

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 and 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 and 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.

D. Deep Learning (MAKA using 3 Factor)

A Bidirectional 3 Layer Security Layer is used with this Algorithm to generate the more secure format on which the proper affects are added to maintain the document secure with CSP Key.

E. Algorithm

Proposed Algorithm In this approach it have consulted two different algorithms and made this new approach.

The approach this algorithm follows is explained below.

- Step 1-When a patient goes to a hospital and is admitted there. The doctor then asks the patient weather he has been attacked by this disease previously or not. If the patient says yes then the doctor enquires which hospital did he went last time.

- Step 2-After getting the hospital name the doctor sends a request to that hospital for getting the patient record. Now It have 2 databases. One will be storing the patient record and other will be storing the public key or in this case the patient's unique CSP key

- Step 3-After searching the database for the provided CSP key the hospital finds the record linked to that key in the record database. Now the hospital sending the record file will encrypt the record by a file key and send it along with the record. The file key in this case happens to be the private key.

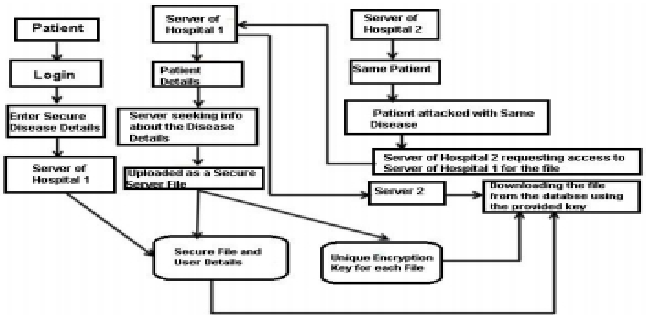
- Step 4-Now to prevent eavesdropping or malicious intermediary attack the file key is also encrypted used hashing function and the variable used is the patient's unique CSP key

- Step 5-First hospital receives the key and the record. First the hospital has to decrypt the file key. Then they can decrypt the record and download it from the server.

In this system It are using two different databases. One database is used to store the record and the other is used to store the private key for decrypting the record. Since It are using asymmetric encryption there will be two keys, one public key and one private key. Now let's suppose a patient comes to a hospital, he is attended by a doctor and the doctor examines the patient and makes a diagnosis of a disease. Now the doctor asks whether he is being attacked by that disease previously the patient denies. So the doctor makes the entry of the patient's record in the database.

Now the patient moves to another town he again gets attacked by the same disease. He goes to a nearby hospital and the doctor examines him and asks whether the patient is being previously attacked by that disease. The patient agrees. Now the doctor will enquire about the hospital the patient went to last time. While the patient record was created the last time a unique CSP key was generated and to access the record the hospital needed to enter the CSP key. Now the second hospital will request the record for the patient with the patient ID. The hospital 1 system will get the request for the record along with the ID of the patient. Now the CSP key is stored in a different database and the record is stored in a different database. Both are linked by record ID. The hospital 1 system will enter the CSP key to send the record. Now after receiving the record hospital 2 will have to unlock it. It will be unlocked by the same private key that will be generated and sent along the record. The private key itself will be encrypted using hashing function and to decrypt it. It will be needing the ID of the patient. Once the key is decrypted the record can be accessed. Now let's see the different enhancements done in our technique. It are using two different databases to store the key and the record. Each key will be linked with the record ID. So for an attacker it is difficult to access the record because then he will be needed to access both the records at the same time as well as he has to know the ID as well as the CSP key. While sending the record even if an attacker intercepts the record he won't be able to open it because it will be protected by a system generated private key.

F. Architecture Diagram


Patient
Login
Enter Secure Disease Details
Server of Hospital 1
Server of Hospital 1
Patient Details
Server seeking info about the Disease Details
Uploaded as a Secure Server File
Server of Hospital 2
Same Patient
Patient attacked with Same Disease
Server of Hospital 2 requesting access to Server of Hospital 1 for the file
Server 2
Downloading the file from the databse using the provided key
Secure File and User Details
Unique Encryption Key for each File

Basic Structural Diagram as mentioned above includes the process:

i. Patient getting admitted to Hospital 1

ii. File for Disease A uploaded successfully

iii. Patient getting admitted in Hospital 2 for same disease

iv. Hospital 2 accessing the file from Hospital 1

v. Generation of CSP Key

vi. Downloading the file through different Authentication and Security Layer

vii. Opening the File with CSP Key

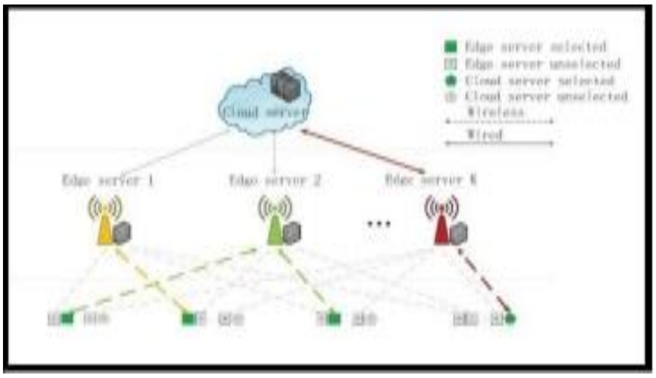
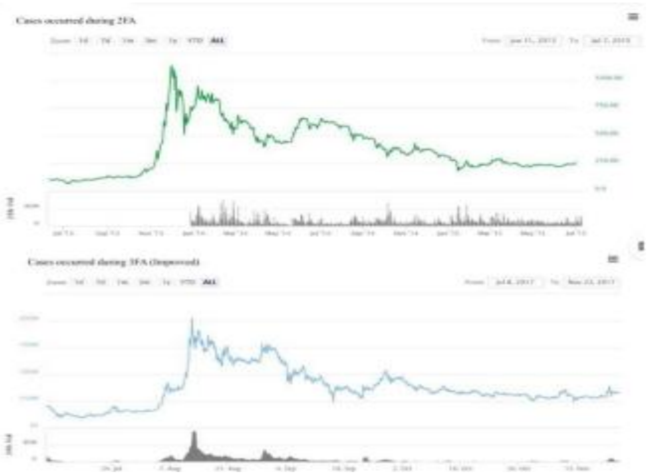


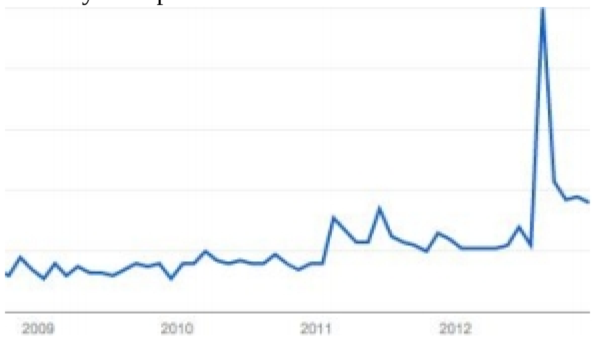
Fig.: Shows the Multiserver Connection for enabling Three Factor Authentication using MAKA Algorithm

IV. RESULTS AND DISCUSSION

A. Dataset and Programming outcome



This Graph shows the outcome before when Two-Factor Authentication was used and compared to the today's situation when we use Three-Factor Authentication and It can be seen properly that The cases which used to be 1000 M all over the world have been reduced to 200 M after we have started using Three Factor Authentication, and It has been improved in a better way using efficiency ion the Algorithm which makes the outcome more secure and trustworthy to implement and use



B. Inference from the Output

The new proposed system uses a much more enhanced version of the existing three factor MAKA protocol. The existing three factor MAKA protocol was complex and difficult to implement and also its implementation required a lot of capital investment. The new enhanced protocol is much simpler, easy as well as cheap to implement. The previous protocol was still vulnerable to intermediary attacks but the proposed protocol has removed this drawback. Since the proposed protocol makes use of two different databases for storing the record as well as the key, the performance increases as compared to the previous proposed protocol. The server load also decreases and the speed of data retrieval also increases. On analyzing our approach and comparing them with other approaches It has graphical proof that our approach is better than the proposed approaches till date. Further It has shown two graphs. One shows the comparisons of computational time based on the number of users. The second one shows the comparison of computation time in multiple servers. Since It are proposing a multi-server protocol it is necessary to show the multi-server time efficiency of our approach.

V. CONCLUSION

Overall the comparison is done with the 2-Factor Authentication and 3-Factor Authentication which is already been introduced, Introducing CSP Key Formation and availability to download and access the file without it, won't be possible is the best thing in this new algorithm, which highly increased the chances that it can be break through to get access through the file.

REFERENCES

1. L. Lamport, "Secret phrase confirmation with shaky correspondence," Communications of The ACM, vol. 24, no. 11, pp. 770–772, 1981.
2. X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Powerful multifaceted confirmation for delicate correspondences," IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 6, pp. 568–581, 2014.
3. He, S. Zeadally, N. Kumar, and J. Lee, "Unknown confirmation for remote body region systems with provable security," IEEE Systems Journal, pp. 1–12, 2016.
4. L. Li, L. Lin, and M. Hwang, "A remote secret word confirmation conspire for multiserver design utilizing neural systems," IEEE Transactions on Neural Networks, vol. 12, no. 6, pp. 1498–1504, 2001.
5. W. Juang, "Proficient multi-server secret word validated key understanding utilizing savvy cards," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 251–255, 2004.
6. C. Chang and J. S. Lee, "A proficient and secure multi-server secret word validation conspire utilizing brilliant cards," in International Conference on Cyberworlds, 2004, pp. 417–422.
7. J.- L. Tsai, "Productive multi-server confirmation conspire dependent on single direction hash work without check table," Computers and Security, vol. 27, no. 3C4, pp. 115–121, 2008.
8. W. Tsaur, J. Li, and W. Lee, "A proficient and secure multi-server validation conspire with key understanding," Journal of Systems and Software, vol. 85, no. 4, pp. 876–882, 2012.
9. Y. Liao and C. Hsiao, "A tale multi-server remote client verification conspire utilizing self- guaranteed open keys for portable customers," Future Generation
10. Computer Systems, vol. 29, no. 3, pp. 886–900, 2013.
11. T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Inspecting smartcard security under the danger of intensity examination assaults," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541–552, 2002.
12. Wang and P. Wang, Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards. Springer International Publishing, 2015.
13. J. K. Lee, S. R. Ryu, and K. Y. Yoo, "Unique mark based remote client verification plot utilizing shrewd cards," Electronics Letters, vol. 38, no. 12, pp. 554– 555, 2002.
14. C. Lin and Y. Lai, "An adaptable biometrics remote client confirmation conspire," Computer Standards and Interfaces, vol. 27, no. 1, pp. 19–23, 2004.
15. C. Chang and I. Lin, "Comments on unique finger impression based remote client verification conspire utilizing shrewd cards," Operating Systems Review, vol. 38, no. 4, pp. 91–96, 2004.
16. H. Kim, S. Lee, and K. Yoo, "Id-based secret key confirmation plot utilizing brilliant cards and fingerprints," Operating Systems Review, vol. 37, no. 4, pp. 32–41, 2003.
17. M. Scott, "Cryptanalysis of an id-based password authentication scheme using smart cards and fingerprints," Operating Systems Review, vol. 38, no. 2, pp. 73–75, 2004.

AUTHORS PROFILE

Mohammad Majid Masroor did his primary and secondary education from St. Joseph's College, Allahabad,Uttar Pradesh and is currently pursuing final year of undergraduate course in Bachelor of Technology from SRM Institute of Science and Technology, Kattankulathur, Chennai,Tamil Nadu. Areas of Interest have always been Defining Algorithms with less complexity.

Kushagra Mishra did his primary and secondary education from The Chintels School, Kanpur,Uttar Pradesh and is currently pursuing final year of undergraduate course in Bachelor of Technology from SRM Institute of Science and Technology,Kattankulathur, Chennai,Tamil Nadu. Areas of Interest has always been a Networking & Data Layer.

Dr. E.Sasikala currently an Associate Professor in Computer Science and Engineering at SRM Institute of Science and Technology, Kattankulathur. She completed her B.Tech in Information Technology at K.S.R. College of Engineering, Anna University, 2006 . Did her Masters of Engineering in Computer Science and Engineering at Anna University of Technology, 2010. She further completed her Doctorate degree in Network Security at Anna University, 2017. She is Life member of the ISTE (Membership Number LM 74419), Annual Member of IET and Annual Member of Indian Science Congress