International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 10 (2017), pp. 2439-2447

http://www.ripublication.com

An Improvised Ibkem Approach Using Multiple Key Distributed For Health Care Application

Dr. V Nagaveni, Thrupthi V.

[1]*Department of Computer Science and Engineering Acharya Institute of Technology, Bangalore, Karnataka, India.*
[2]*Department. of Computer Science and Engineering Acharya Institute of Technology, Bangalore, Karnataka, India.*

Abstract

The main proposal destination of Key- Distribution (K-D)" is to provide competent security to commence with security providing schema in view of smart devices in Cloud generally focalizes on cryptographic method. Reflectance of the IBKEM to our desktop and see through anonymous K-D with one- pass communication providing: "ON-LINE COMMUNICATION: DOCTOR and PATIENT directly communicating to each other by sending the message." "OFF-LINE COMMUNICATION: DOCTOR and PATIENT can even view and access the data through E-mail without accessing to the cloud", this system model suits several instance of health-care services for desktop clients.

Keywords: Real Time Mobile Service, Provable Security; One-Pass Key Distribution; Identity-Based Key Encapsulation Mechanism.

I.INTRODUCTION

Devices unit the conceivable resources that can even sense robust amount of testimony of string of the cloud and jointly possess quality people and ample gauge wherewithal for preeminent operations.

K-D is extremely vital for regulating securitized services and also it had been projected that all the devices implement security network by some of the exploitation suburbanized keys with computationally durable nodes which has abounding tenacious security than trust-relied systems.

Goal is to dispose the headmost interrogation once needed is update S-K time to time repeatedly conflicts with the decisive though key price would be straight line with respect to the amount of obtainer by key agreement.

II. SYSTEM ARCHITECTURE

There are 4 main parties which is been discussed below:

- "TTP is the system organizer, it takes all the AU system details and generate some random parameters with this parameter only SK is obtained."
- "Manager mostly responsible for distribution of SK to the corresponding AU and it would be distributed to both Doctor and Patient, and their uploaded tested report by the moderator of the patients would be in readable format, however it is responsible for AU communication."
- "AU receives SK, only by accessing this SK AU can enter in to the application, fetch reports and communicate."
- "The cloud primarily quoted as storage of report, hence the tested report undergoes transformation from the Moderator to Doctor/Patient."
- Step1: MODERATOR has to login by giving his {NAME, E-MAIL ADDRESS and PHONE NUMBER}.
- Step2: Moderator would be getting the SK from the cloud itself, as he also has option to change the password according to his needs.
- Step3: After login he would upload test report for both Doctor and Patient while in this process the uploaded report initially would be stored in the encrypted format in the cloud server.
- Step4: Only after the registration of Doctor and Patient in the application can download the report from the cloud server which would be in decrypted format, as shown below in the Fig 1:

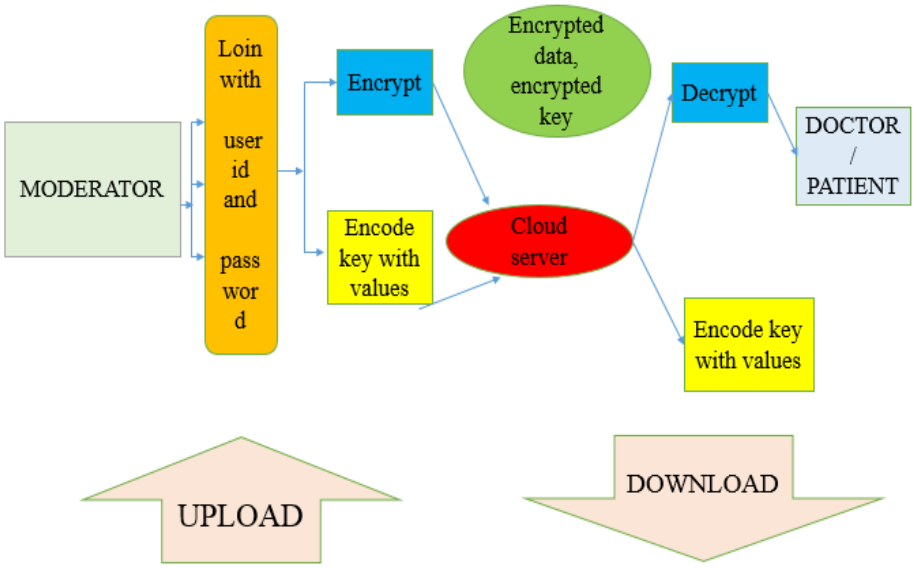


Figure 1: System Architecture

III. DETAILED WORKING

Detailed working process of each entity is been shown in sequence diagram Fig 2:

Step1: DOCTOR/PATIENT login to cloud server. Step2: Verification in cloud server.

Step3: Entering of details.

Step4: Checking for password in E-mail. Step5: Updating new password.

Step6: MODERATOR logged in.

Step7: Cloud server response to MODERATOR.

Step8: Upload testing report to both DOCTOR/PATIENT. Step9: While cloud server stores report, by using AES 256 algorithm converts tested report to encrypted format.

Step10: Updating in to the database, here MYSQL comes in to play.

Step11: DOCTOR/PATIENT request for the tested report. Step12: MODERATOR logged out from cloud server. Step13: DOCTOR/PATIENT can download file to watch the report.

Step14: DOCTOR and PATIENT can communicate to each other.

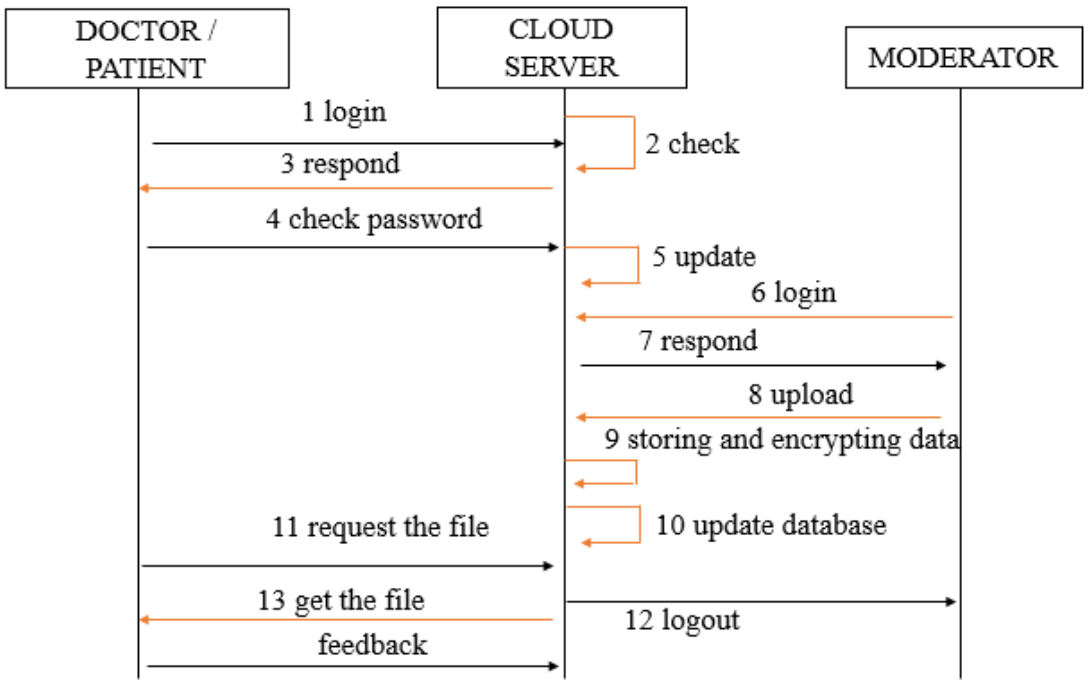


Figure 2: Detailed Sequence Diagram

IV. RESULTS

A. DOCTOR LOGIN PAGE

Initially user 1 = DOCTOR login format where he would be providing some of his details like {name , e-mail address , phone number} and press sign in button as shown in the Fig 3.

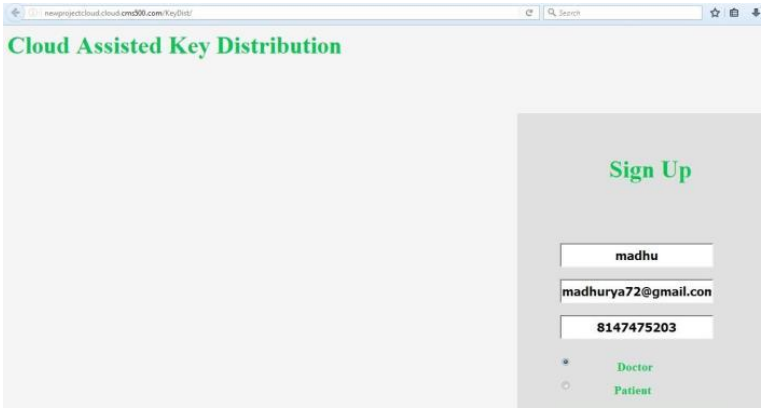


Figure 3: Doctor Registration

B. SESSION KEY GENERATION OF DOCTOR

After the registration of the doctor the session key as user password would be generated in the e-mail therefore stronger security is been provided. As this session key would be randomly generated by the cloud whose length is 8byte in hexadecimal as shown in Fig 4.

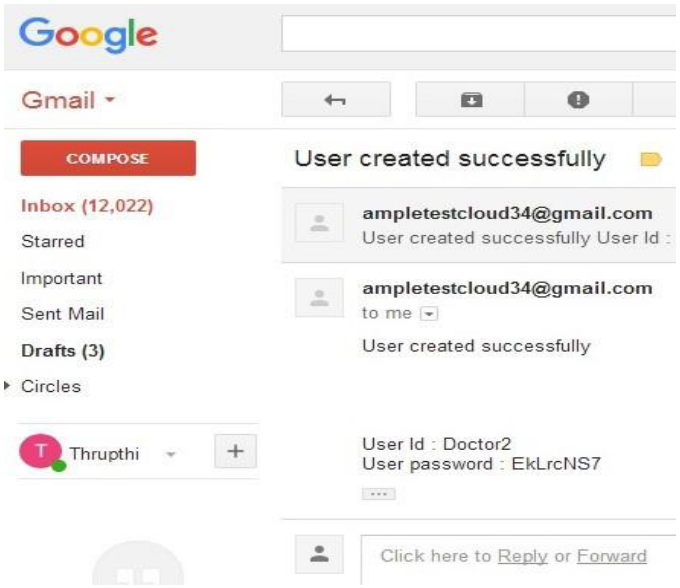


Figure 4: Session Key Generation

C. LOGGED IN PAGE DOCTOR

After the process would be getting logged in page as shown in the Fig 5, which consist of some details like: Owner f the account name example: MADHURYA. Download file: In this option we can download any kind of files example: PDF file, image file, doc file, txt file. For text file there is no size limitation.

Communicate: In this option Doctor can communicate or send any message regarding the report of the patient and also can view the patient message to that report.

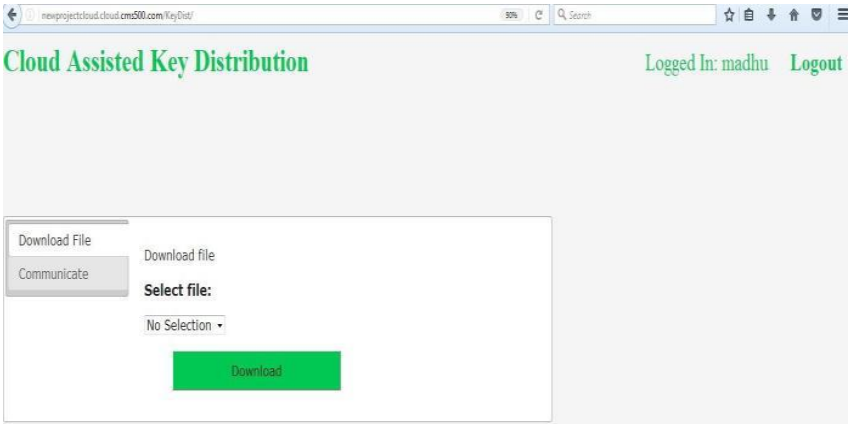


Figure 5: After Entering the New Password

D. PATIENT LOGIN PAGE

Initially user 2 = PATIENT login format where he would be providing some of his details like {name , e-mail address , phone number} and press sign in button as shown in the Fig 6.

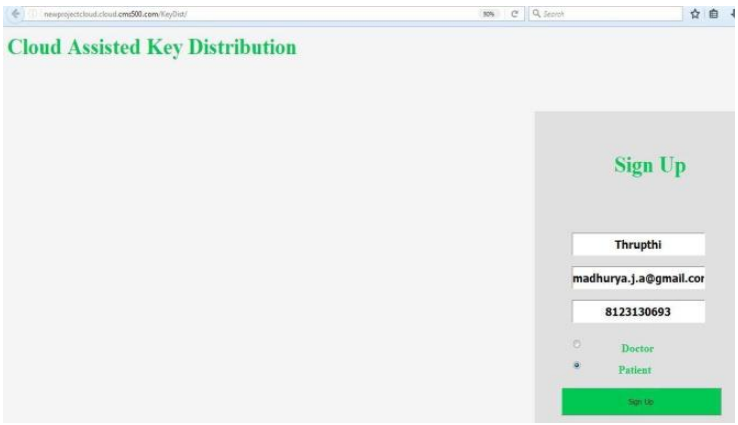


Figure 6: Patient Sign Up

E. SESSION KEY GENERATION OF PATIENT

After the registration of the patient the session key as user password would be generated in the e-mail therefore it provides stronger security. As this session key would be randomly generated by the cloud whose length is 8byte hexadecimal as shown in the Fig 7.

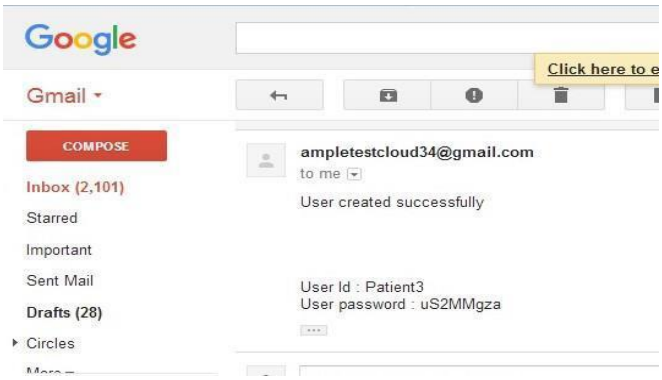


Figure 7: Patient Session Key Generation

F. LOGGED IN PAGE PATIENT

After the process would be getting logged in page as

- Shown in the Fig 8, which consist of some details like: Owner of the account name example: THRUPTHI. Download file: In this option we can download any kind of files example: PDF file, image file, doc file, txt file. For text file there is no size limitation.
- Communicate: In this option patient can communicate or send any message regarding the report of the patient, also can view the doctor remarks or message on the report.

Figure 8: PATIENT LOGIN VIEW

G. MODERATOR OPERATION

MODERATOR LOGIN'S and can see the login page shown in the Fig 9 and it consist of operation activity list like:

- Owner of the account name example: MODERATOR.
- UPLOAD FILE: MODERATOR can upload any type of file example: PDF file, doc file, text file, image file.
- Select DOCTOR: This is to select to which doctor he has to send files example: MADHURYA.
- Select PATIENT: This is to select to which patient he has to send files example: THRUPTHI.

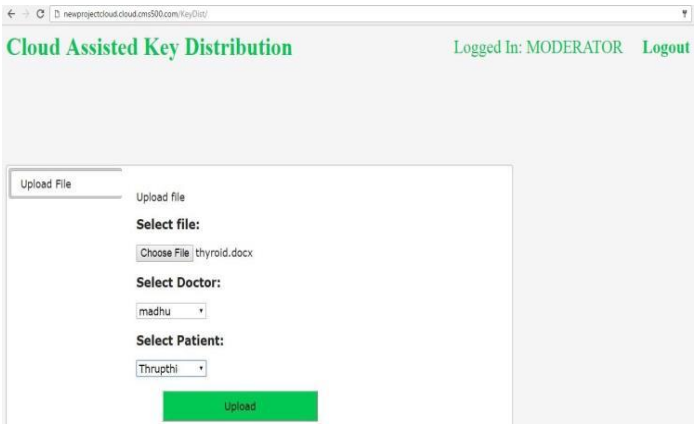


Figure 9: Moderator Process

H. GRAPH

Graph plotting represents the time taken for encryption of each report would be displayed as shown in theFig 10.

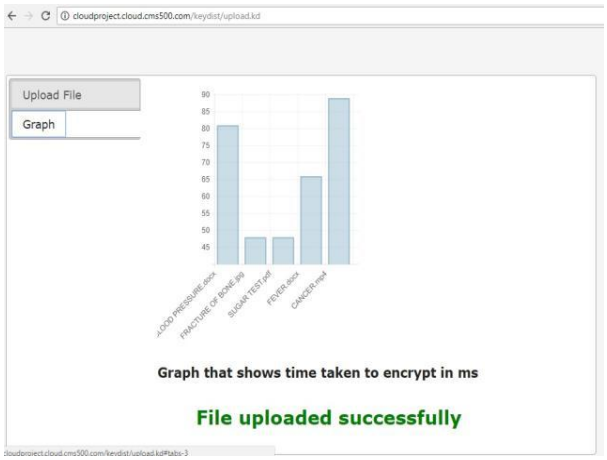
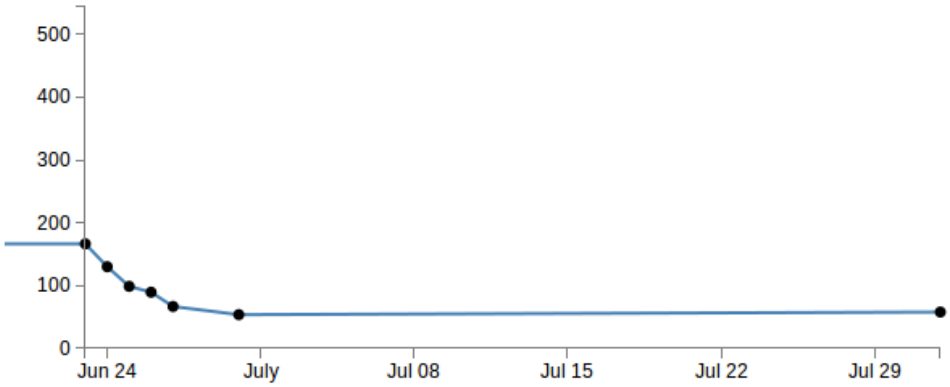


Figure 10: Graph

I. COMPARISION OF IMPROVEMENT IN PROJECT

Comparison of seven different papers results with the proposed paper, we can observe the efficiency increased and the time take is lesser.



V. CONCLUSION

Usage of advanced IBKEM techniques for WSN increases efficiency and generation of private keys and session key , without affecting time complexity usage of AES 256 algorithm increase the confidence of the desktop clients about the communication and also there data increase number of receiver which leads to decrease in usage of time compact and the capacity of data base. Providing on-line communication application: DOCTOR and PATIENT communicating directly to each other by sending the message and off-line communication facilities to Client's application: DOCTOR and PATIENT can even view and access those data through e-mail without accessing to the cloud, this system model suits several instances of health- care services.

REFERENCES

[1] Cloud-Assisted Key Distribution in Batch for Secure Real-time mobile Services Wei Wang, Member, IEEE, Peng Xu, Member, IEEE, Laurence Tianruo Yang, Senior Member, Senior Member, IEEE-2016 .

[2] Wei Wang, Peng Xu and Laurence Tianruo Yang. One-Pass Anonymous Key Distribution in Batch for Secure Real-Time Services. In: 2015 IEEE International Conference on Services.

[3] Leonardo B. Oliveira, Diego F. Aranha, Conrado P. L. Cmara, Julio Lpez and Ricardo Dahab. TinyPBC: Pairings for Authenticated Identity- based Non-interactive Key Distribution in Sensor Networks. Computer Communications, 34(3), pp. 485-493, 2014.

[4] Peng Xu, Tengfei Jiao, Qianhong Wu, Wei Wang, Hai Jin. Conditional Identity-based Broadcast Proxy Re-Encryption and Its Application to Email.

[5] Noel McCullagh and Paulo S.L.M. Barreto. A new two-party identity- based authenticated key agreement. Topics in Cryptology-CT-RSA 2005, LNCS 3376, pp. 262-274, Springer, Heidelberg, 2015.1