SECURING INFORMATION IN CLOUD ASSISTED HEALTH MONITORING SYSTEM USING BLIND STORAGE

[1] Mr. Suyog S. Dhoot, [2] Prof. K. N. Shedge, [3] Mr. Girish. R. Shinde
[1,3] Department of Computer Engineering, SVIT, Chincholi, Maharashtra
[2] HOD, Department Computer Engineering, SVIT, Chincholi , Maharashtra2
sdhoots@gmail.com

Abstract— Cloud based health monitoring system is new approach to focus on immediate health solution for remote areas. This technique will be useful as number of smartphone user are more now and network availability is good. While considering security of user information an implemented technique or scheme will provide secure computing using AES character encoding technique and blind search encryption technique. Heath service provider will get new digital market to grow up business and will store there branching health program in encrypted form. Secure shell through remote method invocation and sandmark tool will provide security to digital information. Decryption technique through secure code will add extra security to suggestive action obtained from service provider through cloud. Efficiency of implemented project is good as it access by mobile app and get solution within time.

Keywords— Branching Tree, Health Service Provider, Blind Storage, Outsourcing Decryption, Character Encoding.

I. INTRODUCTION

The most important aspect of human life is its health. Remote health monitoring system which is operated through mobile phones or wireless network is important aspect in the field of technology and adopted by developing countries. In remote areas of Caribbean countries Microsoft launched project “MediNet” i.e. health monitoring feedback decision system for diabetes and cardiovascular diseases. User give its health related information as input which passes through web based medical application programs to give decision or feedback or precaution to user based on program is set. It provide good market sector for health service provider to deliver its service to user for various deceases. User can select their medical health service provider based on privacy of information and efficient computing provide by them. Health service provider operated through cloud so that less setup cost is required and user can access this system from anywhere and also user get output at low cost so user acceptances will also increase. Due to involvement of cloud more work will performed by cloud and less computational work done at user, health service provider side. In order to move towards a developing nation this type of systems are very useful to maintain the health of peoples which lived in remote areas. Government can take initiative in budget allocation which will be needful project in the field of medical, health science. Cloud based health monitoring system is useful system but security or privacy of information is important factor while design this type of system. Maintaining privacy of user information which contains sensitive data regarding their health status is required at high level. Information may be breached at different operations like storing, monitoring, applying, communicating etc. A survey shows that majority of people are very careful about privacy of their health information. User is not ready to adopt this type of system as they think that the information which is passed through electronic or wireless media can be break or tackled at any level of operation. In order to make effective system privacy of user information is very needful so that large number of peoples gets involved in such systems. Existing rules, regulations, laws, standards that are set by regulating agencies and standard creation committees are applicable for only static record system and not considered for cloud based environment. Some laws are put limitations on cloud to maintain security of user information but not provide any constraint on health service provider.

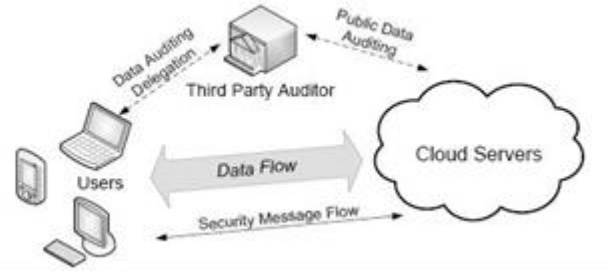


Fig-1: Architecture of Cloud Data Storage Service

II. SURVEY REVIEW

- Johannes Barnickel, Hakan Karahan, Ulrike Meyer proposed a system for security and privacy architecture and implementation of the HealthNet mobile electronic health monitoring and data collection system. Privacy and security is achieved through data avoidance, data minimization, decentralized storage, and the use of cryptography. This system does not deal with centralized approach where as health service provider program does not secure.

- Rifat Shahriyar, Md. Faizul Bari, Gourab Kundu, Sheikh Iqbal Ahamed, and Md. Mostofa Akbar proposed Intelligent Mobile Health Monitoring System (IMHMS) for improving communication among patients, physicians, and other health care workers. Security in IMHMS is provided by using RFID. Each patient will be provided RFID tags that will be used to uniquely identify the patient. The IMS will maintain patients profile information with the RFID in the central database. So malicious attacks can be blocked using this information because a patient can be easily tracked using RFID. As it require large memory and cost so high computational complexity required to secure user personal information from unauthorized access.

- Minho Shin, Research Article on Secure Remote Health Monitoring with Unreliable Mobile Devices in which he provided risk analysis and present a framework for secure remote health monitoring systems. We also designed a health monitoring architecture that leverages a special monitoring unit that plays the central role of the security by providing critical security services including authentication, audit, key management, and data fusion. This system does not concerned regarding security of health service provider and more records are required for monitoring program.

- D. D. Kouvatsos, G. Min and B. Qureshi research on Performance Issues in a Secure Health Monitoring Wireless Sensor Network. It concerned with Data Privacy at acquiring level, Data security at transmission level, Data security at healthcare provider level. In that therefore a new secure transmission protocol is required providing optimal transmission control and bandwidth utilization to incorporate multimedia (audio / video) data.

- BENJAMIN C. M. FUNG, KE WANG, RUI CHEN, PHILIP S. YU present A Survey of Privacy-Preserving Data Publishing which state that detailed person-specific data in its original form often contains sensitive information about individuals, and publishing such data immediately violates individual privacy.

- D. Kavitha proposed preserving text search privacy through blind storage towards secure storage and retrieval of data. The blind storage is to preserve the outsourced data in cloud through gateway encryption and to implement multi-keyword ranked search over the encrypted data in a secure way by NLP process without downloading and decrypting the entire group member file contents.

III. EXPERIMENTAL SETUP

New approach for cloud based health monitoring system consist of three components or parties i.e. User at client side, Cloud server, cloud server and health service provider. After initialization health service provider will store there medical application program in the form of branching tree in cloud. This branching tree is encrypted and generated cipher text is stored in cloud using AES character encoding encryption technique. To identify service provider, each service provider gets one index and along with that index encrypted branching tree program stored in cloud. When particular user wants decision or feedback from service provider it starts token generation operation .Client sends index value of health service provider along with its input value vector which consists of user health information. User input query passed in the form of vector with information components. After getting input query from Client sends token to cloud server which require for getting decision. Cloud will validate tokens and cloud send this token to health service provider then service provider will generate feedback or decision based on decision tree structure and it was passes to cloud in cipher text format. Cloud will get partially decrypted cipher text which pass to client using blind search or blind storage encryption technique. As this is partially message so cloud not get any useful information of decision or feedback.

Figure 2 shows the architecture of proposed system. An advance system which uses secure key duplicate 2-way encryption for security and efficiency in which 2 ways encryption is done. It also reduces computational workload at user side and move to cloud. During initialization third party auditor initializes and run setup phase and it generates system required parameter. For outsourcing decryption a secure code sends to user email address. After entering secure code, a user can get decrypted cipher text.

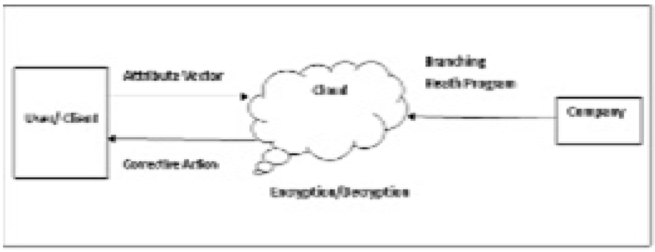
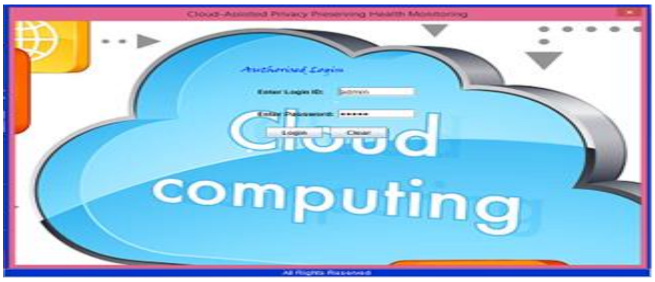


Fig-2: Architecture of Implemented System

IV. IMPLEMENTATION

Final implemented project starts with server connection. After starting server a health service provider will upload health service program in the form of branching tree on cloud. This program will be in encrypted form. Following is screenshots of implemented module.



Cloud-Assisted Privacy Preserving Health Monitoring

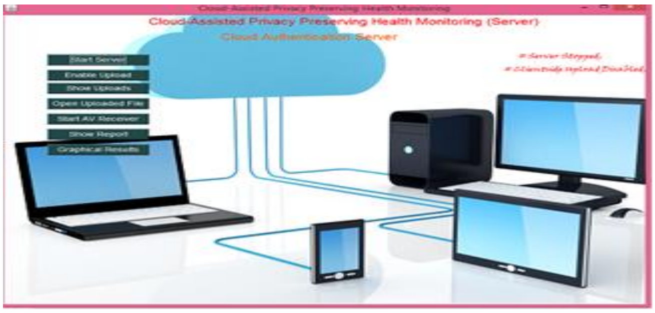
Authorised Login

Enter Login ID: admin

Enter Password: *****

Fig- 3: Login Page for Cloud/ Server

Figure 3 shows login page through which cloud or server will started. Unless and until server started it was impossible to run any application by user or health service provider.



Cloud-Assisted Privacy Preserving Health Monitoring

Cloud-Assisted Privacy Preserving Health Monitoring (Server)

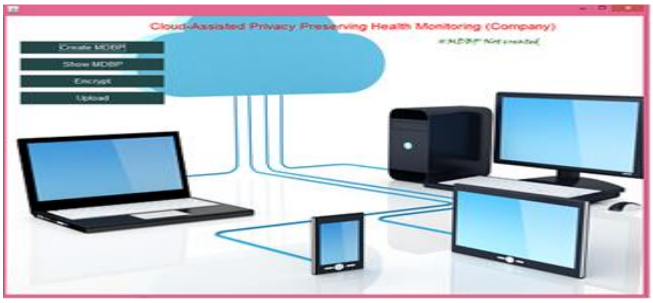
Cloud Authentication Server

Server Stopped.

Clientside Upload Disabled.

Fig-4: GUI of Cloud Module

Figure 4 shows GUI of cloud module with different functionality. It has enable upload, show upload option through which health service provider i.e. company will upload there branching program on it. It also has option to start receiving attribute vector i.e. user input query. Cloud can also view results based on number of computation and user.

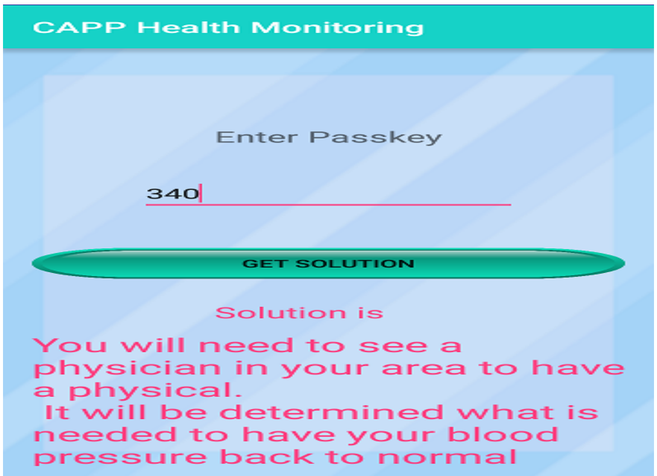


Cloud-Assisted Privacy Preserving Health Monitoring (Company)

MDBP Not created

Fig-5: GUI of Health Service Provider Module

Figure 5 shows GUI of health service provider i.e. company module. It has different functionality like creation of medical database program, creation of branching program, encryption of self-created program and upload option. Branching program for different diseases for different parameters are created by health service provider. After that user login page will opened. User will login himself through android app after performing registration. After login by user, user will select symptom from given list for particular disease. This information passes in the form of token to cloud.



CAPP Health Monitoring

Enter Passkey

340

Solution is

You will need to see a physician in your area to have a physical.
It will be determined what is needed to have your blood pressure back to normal

Fig-6: Outsourcing Decryption

Figure 6 show that user has to pass the passkey which is a secure code pass to user email id. After entering correct pass key a solution or feedback received by user from cloud.

V. RESULTS

Security and Efficiency are two major outputs of implemented project. Security is achieved by using AES character encoding encryption algorithm. Health service program of company is secured in cloud as it provide sensitive output to user. Cloud or health service provider will not get any personal or medical information of user. Security of data is achieved by user due to use of blind search technique to search data in encrypted data. This implemented scheme will provide solution to secure from insider and outsider attack in cloud. Due to use of outsourcing decryption through secure code on email no data can be read by outsider person due to ciphertext. As decryption done by user so less computation required at cloud or server side. User getting the reply timely by providing a active connection with server and accurately. Efficiency depends on sensor through which input information of client is passed, internet connection and quality of smartphone. Sometime user not getting response quickly due to different parameters or network issue but in normal efficiency of implemented scheme is good. An testing of n number of user with different interval and m number of computation was done which proves implemented project is secure and efficient.

CONCLUSION

Cloud based health monitoring system efficiently secure privacy of user information and application programs of health service provider. To maintain privacy of user information in cloud and from insider attack, AES character encoding encryption technique is used to deals with personal identifiable information. Outsourcing decryption technique will reduce computational overhead at user side and move to cloud. Branching program are encrypted using different branch node values for maintaining security of that. By applying newly developed blind storage scheme computational overhead at service provider side will reduce so small organization or companies can take participation in business and create their market in efficient way. Security and Effectiveness are achieved through implemented scheme.

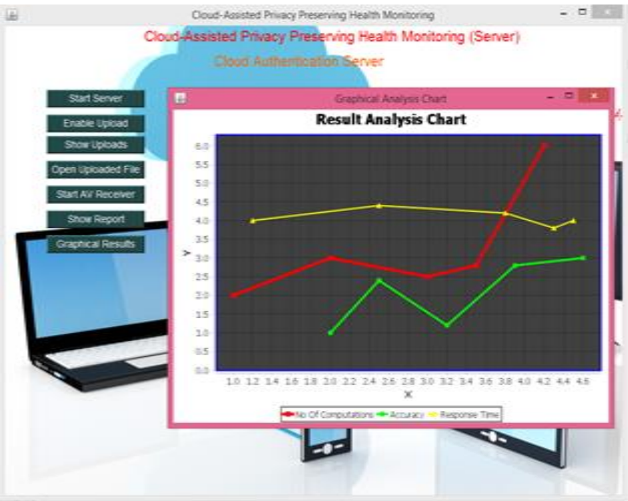


Figure 7: Graphical Result Analysis

References

[1] Huang Lin, Jun Shaoy, Chi Zhangz, Yuguang Fang, fellow IEEE," CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring." IEEE TRANASCTIONS ON IMAGE PROCESSING VOL: 8 NO: 6 YEAR 2013.

[2] P. Mohan, D. Marin, S. Sultan, and A. Deen, "Medinet: personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony." Conference Proceedings of the International Conference of IEEE Engineering in Medicine and Biology Society, vol-2008.

[3] A. Narayanan and V. Shmatikov, "Myths and fallacies of personally identifiable information," Communications of the ACM, vol. 53, no. 6, pp. 24–26, 2010.

[4] J. Brickell, D. Porter, V. Shmatikov, and E. Witchel, "Privacy-preserving remote diagnostics," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 498–50

[5] Cong Wang, Student Member, IEEE, Sherman S.M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE, "Privacy-Preserving Public Auditing for Secure Cloud Storage."

[6] G. Clifford and D. Clifton, "Wireless technology in disease management and medicine," Annual Review of Medicine, vol. 63, pp. 479–492, 2012.

[7] E. Shi, J. Bethencourt, H. T.-H. Chan, D. X. Song, and A. Perrig, "Improve Security and Search over Encrypted Cloud Data Using Blind Storage and Gateway Encryption," in IJARTET, 2016, pp. 691–695.

[8] Johannes Barnickel, Hakan Karahan, Ulrike Meyer, UMIC Research Center," Security and Privacy for Mobile Electronic Health Monitoring and Recording Systems."

[9] P. Dixon, "Medical identity theft: The information crime that can kill you," in The World Privacy Forum, 2006, pp.13-22.

[10] D. D. Kouvatsos, G. Min and B. Qureshi, "Performance Issues in a Secure Health Monitoring Wireless Sensor Network."

[11] W. Stallings, "Cryptography and Network Security: Principle and Practices", Prentice Hall.