INTERNATIONAL JOURNAL OF
TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

Cloud-based Fine-grained Health Information Access Control Framework for Lightweight IoT Devices with Dynamic Auditing and Attribute Revocation

DEVARAKONDA VENKATA RAMYA
PG Scholar, Department of M.C.A,
S.K.B.R P.G College,
Amalapuram, E.G.Dt., A.P, India.
venkataramyadevarakonda123@gmail.com

Mr. NAGA. SRINIVASA RAO*
Asst. Professor, Dept of M.C.A,
S.K.B.R P.G College,
Amalapuram, E.G.Dt., A.P, India.
E-Mail:naagaasrinu@gmail.com

***Abstract* --**
In the literature, we in the healthcare sector have witnessed the growing demand for and acceptance of software development in the cloud environment to address and meet current and future healthcare service needs. In this white paper, we propose a flexible, secure, cost-effective, and secure cloud-based healthcare framework. We propose a secure and efficient framework for the government's EHR system in which fine-grained access control based on multi-agency ciphertext attribute-based encryption (CP-ABE) can be enabled along with a hierarchical structure for enforcing access control policies. The proposed framework will allow decision-makers in the Kingdom of Saudi Arabia to develop the healthcare sector and benefit from the existing Yasser e-government cloud computing platform, which is responsible for delivering common services through a highly efficient, reliable and secure environment. This framework aims to provide government health services and facilities to citizens (G2C). In addition, a multi-level applicant authentication was identified and proven in cooperation with two trustworthy bodies. Security analyzes and comparisons with the corresponding frameworks were carried out.

Index Terms: **Cloud storage, fog server, Xor-Combination, CRH, privacy.**

I. Introduction

A widespread public health phenomenon in most Arab countries is the lack of optimal use of available human and material resources to provide integrated health care to prevent diseases and treat diseases after they have occurred. Statistics show that Arab countries suffer from high rates of health problems like diabetes, liver disease, and parasitic diseases like histosomiasis and malaria. These health problems could be prevented before they occur or their complications prevented with early detection. This is due to a combination of factors: planning, operation and engineering. If we could overcome them, it would lead to significant advances in healthcare. In addition, there is a weakness and lack of hospital information systems available, which are among the most advanced software that directly serves all technical and administrative health activities, ensuring that the medical institution has full control over all its activities and resources. The success of these advanced systems does not depend on the precise choice of storage devices and software. Rather, their success depends on their suitability for different healthcare provider users such as doctors, nurses,

technicians and even administrators, where the vision and priorities of each of these categories differ and their information needs and benefits of each of these systems are different. The traditional health care system (paper) has been replaced by an electronic health information system as the traditional system has proven to be ineffective due to a number of problems including low storage. The computerized healthcare system was then replaced by cloud computing due to its reliance on more efficient infrastructure as
reduces costs in the provision of health services, maintenance costs, networks, other features [2]. The use of cloud computing in electronic medical records license fees and infrastructure in general and will therefore encourage developers to use the cloud in healthcare [2], [3]. well as the many benefits of cloud computing in IT such as cost, scalability, flexibility, and
The rapid shift to the cloud and their use in healthcare systems has raised concerns about crucial privacy and information security issues [4], [5]. Adoption of the cloud in IT increases healthcare providers' focus and concern for clinical and patient-related services and decreases attention to infrastructure management [6].

II. Related Work

There are no existing powerful frameworks that clearly address all viable schemes and interrelationships between cloud computing and health technology. Improving the healthcare framework in cloud computing has been studied by several researchers. Further developments and solutions to these challenges will drive adoption of cloud healthcare and encourage healthcare providers to move forward with cloud-based services.

The exchange of personal and health information over the internet and various servers outside of the secure environment of the healthcare facility has created a number of privacy, security, access and compliance issues [7], [8], [9], [10]. There are no existing powerful frameworks in the literature that clearly address all feasible schemes and interrelationships between cloud computing and health technology.

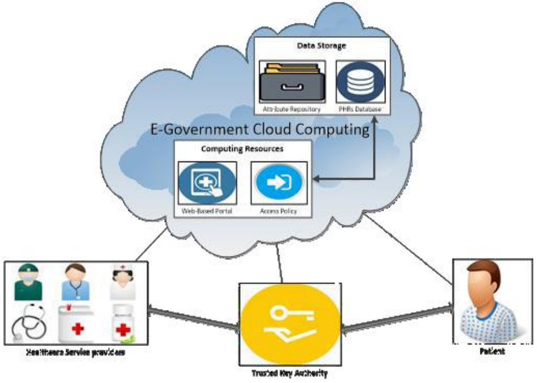
Our contributions can be summarized as follows:

➢ Provides a flexible, secure, cost-effective, and privacy-protected G-Cloud-based framework for government healthcare services through:

- Apply, use and modify the latest encryption and decryption mechanisms suitable for cloud-based EHR systems. The proposed scheme does not use the default encryption system, which is not suitable for the cloud environment.
- Achieving the scalability of computing resources that can be expanded and controlled according to the healthcare services required. The EHR is capable of supporting massive data exchanges.
- Providing an effective solution for government healthcare decision-makers to adopt cloud-based healthcare systems, particularly in developing countries. Providing better authentication Multi-factor applicant authentication in cooperation with two trusted authorities. Different domains of attributes are managed by different attribute authorities that operate independently and are controlled by the central trusted authority. The security analysis was carried out according to the most important security requirements in cloud environments.

III. THE PROPOSED GCLOUD-BASED FRAMEWORK

The proposed framework uses cloud computing to develop health services that the Ministry of Health offers to citizens. This framework aims to provide health services and facilities from the government to the citizens (G2C) in the Kingdom.



The Proposed G-Cloud-Based Framework

1. The Patient

The patient is the main entity in our proposed framework. The patient has the following main tasks:

- A new patient must submit an authentication request to the trusted authority to obtain his or her identification number (ID) and then he or she can use the system services.
- Creates the patient record (PHR) and stores it on the cloud server.
- Ensures the PHR is fully secured and protected by defining an (attribute-based) access policy that can be used to encrypt the data before it is distributed.

2. *Healthcare Providers*

Healthcare providers are individuals who provide healthcare services of all kinds in an organized manner to all members of a community. Healthcare providers could include the following members: naturopaths and medical specialists, physicians, nurses, pharmacists, surgeons, medical technicians, laboratory technicians, and other employees. Each of these members must have access to a portion of patient records for specific purposes.

Each healthcare provider must complete the following tasks:

- Obtain an identification number (ID) from the trusted authority to access certain parts of the patient's record.
- Apply a request for the secret key appended with the appropriate parameters.
- Be able to decrypt, modify and encrypt the same document with the same key.

3. *Trusted Authority*

The trusted authority (TU), such as the Ministry of Health or any government sector, is responsible for the following functions:

- Authenticate all participants interacting with the system.
- Generate keys for healthcare providers and publish public parameters required for cryptographic operations.

4. *The E-Government Cloud-Based EHR*

The cloud-based eGovernment EHR is the backbone of our proposed framework. In the Kingdom of Saudi Arabia, the eGovernment program (Yesser) was established and one of its initiatives and products is Government Cloud Computing. This government cloud computing provides beneficiaries with an efficient, secure, and reliable infrastructure, platform, and software, all as services.

The proposed e-government cloud-based EHR consists of the following cloud services:

- The first service consists of two basic parts: data repository and computing resources. The first service is responsible for storing the encrypted EHRs, which only the authenticated healthcare providers can access via an access policy based on the healthcare provider's attributes.
- The second service is responsible for generating the access policies, providing

ISSN: 2057-5688

efficient key management, and performing other necessary computations.

- The third service hosts the web-based portal. The developed web-based portal should be a secure online website that shareholders can access from anywhere, with 24 hours a day access, with an internet connection and accessible from any device.

The proposed scheme consists of the following five algorithms:

1. Setup (K). The system setup algorithm takes a security parameter, K, as input. It outputs the public key (PK) and the master key (MK).
2. CreateAttributeAuthority (PK, AA). This algorithm is executed by the GA (central authority) with the AA request as input. It outputs a functional identifier, Aid, for the AA with a set of attributes, Sid, and a secret authority key, SKAid. The Ministry of Health categorizes the AAs according to their functionalities and then assigns the attributes for users of these functionalities.
3. AttributeKeyGenerator (PK, SKAid, Sid). This algorithm is executed by the Aid domain authority. It takes as input the PK and the domain authority's secret key, SKAid, and the set of attributes, Sid. It outputs the attribute secret keys for the user SKUj.
4. Encrypt (PK, M, P, PKU). The encrypt algorithm takes as input the PK, a message (M), an access policy (P), and the set of public user keys (PKUs) corresponding to all the attributes in P. It outputs the ciphertext message CT.
5. Decrypt (PK, CT, P, SKUj, SKA). The decrypt algorithm takes as input the PK, a ciphertext message CT, the same access P used in encryption, the secret user key, SKUj, and the set of secret attribute keys, SKA. The CT message will be decrypted if the attributes are sufficient to satisfy the P; otherwise the output will be null.

IV. SECURITY ANALYSIS

The proposed CP-ABE framework for multi-attribute hierarchical authorities in the EHR cloud environment meets the following security requirements:

❖ **Data privacy**

The proposed framework protects users' privacy. The EHR's privacy is satisfied when the user uploads the message encrypted with the access policy privileges settled by the user's own policy and is protected by authority attribute domains.

❖ **Fine-grained access control**

The proposed framework is designed in such a way that after successful identity authentication, different subjects have different access rights according to the attribute key generator and the access policy used by the user. The proposed framework is based on CP-ABE [21] and uses a central authority with multiple authority attribute domains imposing different access rights for different types of applicants to achieve fine-grained access control. This means that all attributes must be checked against the user access policy structure in order to access the required information.

❖ **Efficiency**

The amount of computation done by the government or the central authority can be greatly reduced by assigning tasks to the attribute area authorities. The proposed scheme enforces attribute domain authorities for generating and distributing keys to the entities. In general, applying multiple attribute domain authorities can efficiently distribute computational effort across multiple domain authorities because each authority is not overloaded.

V. CONCLUSION AND FUTURE WORK

We proposed a secure cloud-based EHR framework that guarantees the security and privacy of medical data stored in the cloud and relies on hierarchical CP-ABE with multiple agencies to enforce access control policies. The proposed framework provides a high level of integration, interoperability and sharing of EHRs between healthcare providers, patients and physicians. In the framework, the attribute domain authority manages another attribute domain and works independently. The computational effort is taken care of by the government agency and the multi-factor applicant authentication has been identified and proven.

The proposed system can be adopted by any government that has cloud computing infrastructure and offers treatment services to the majority of citizen patients. Future work includes implementation and evaluation of the proposed scheme in a real environment.

REFERENCES

1. Improving product marketing by predicting early reviewers on E-Commerce websites
S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, “Improving product marketing by predicting early reviewers on E-Commerce websites,” Deleted Journal, no. 43, pp. 17–25, Apr. 2024, doi: 10.55529/ijrise.43.17.25.

2. Kodati, Dr Sarangam, et al. “Classification of SARS Cov-2 and Non-SARS Cov-2 Pneumonia Using CNN.” Journal of Prevention, Diagnosis and Management of Human Diseases (JPDMHD) 2799-1202, vol. 3, no. 06, 23 Nov. 2023, pp. 32–40, journal.hmjournals.com/index.php/JPDMHD/article/view/3406/2798, https://doi.org/10.55529/jpdmhd.36.32.40. Accessed 2 May 2024.

3. V. Srikanth, “CHRONIC KIDNEY DISEASE PREDICTION USING MACHINE LEARNING ALGORITHMS,” IJTE, pp. 106–109, Jan. 2023, [Online]. Available: http://ijte.uk/archive/2023/CHRONIC-KIDNEY-DISEASE-PREDICTION-USING-MACHINE-LEARNING-ALGORITHMS.pdf

4. V. SRIKANTH, “DETECTION OF PLAGIARISM USING ARTIFICIAL NEURAL NETWORKS,” International Journal of Technology and Engineering, vol. XV, no. I, pp. 201–204, Feb. 2023, [Online]. Available: http://ijte.uk/archive/2023/DETECTION-OF-PLAGIARISM-USING-ARTIFICIAL-NEURAL-NETWORKS.pdf

5. V. SRIKANTH, “A REVIEW ON MODELING AND PREDICTING OF CYBER HACKING BREACHES,” IJTE, vol. XV, no. I, pp. 300–302, Mar. 2023, [Online]. Available: http://ijte.uk/archive/2023/A-REVIEW-ON-MODELING-AND-PREDICTING-OF-CYBER-HACKING-BREACHES.pdf

6. S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, “Detection of fake currency using machine learning models,” Deleted Journal, no. 41, pp. 31–38, Dec. 2023, doi: 10.55529/ijrise.41.31.38.

7. “Cyberspace and the Law: Cyber

Security." IOK STORE, iokstore.inkofknowledge.com/product-page/cyberspace-and-the-law. Accessed 2 May 2024.

8. "Data Structures Laboratory Manual." IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-structures-laboratory-manual. Accessed 2 May 2024.

9. Data Analytics Using R Programming Lab." IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-analytics-using-r-programming-lab. Accessed 2 May 2024.

10. V. Srikanth, Dr. I. Reddy, and Department of Information Technology, Sreenidhi Institute of Science and Technology, Hyderabad, 501301, India, "WIRELESS SECURITY PROTOCOLS (WEP,WPA,WPA2 & WPA3)," journal-article, 2019. [Online]. Available: https://www.jetir.org/papers/JETIRDA06001.pdf

10. V. SRIKANTH, "Secured ranked keyword search over encrypted data on cloud," IJIEMR Transactions, vol. 07, no. 02, pp. 111–119, Feb. 2018, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/1121_approvedpaper.pdf

11. V. SRIKANTH, "A NOVEL METHOD FOR BUG DETECTION TECHNIQUES USING INSTANCE SELECTION AND FEATURE SELECTION," IJIEMR Transactions, vol. 06, no. 12, pp. 337–344, Dec. 2017, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/976_approvedpaper.pdf

12 . SRIKANTH MCA, MTECH, MBA, "ANALYZING THE TWEETS AND DETECT TRAFFIC FROM TWITTER ANALYSIS," Feb. 2017. [Online]. Available: http://ijmtarc.in/Papers/Current%20Papers/IJMTARC-170309.pdf

14 Srikanth, V. 2018. "Secret Sharing Algorithm Implementation on Single to Multi Cloud." International Journal of Research 5 (01): 1036–41. https://journals.pen2print.org/index.php/ijr/article/view/11641/11021.

5. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21, https://doi.org/10.55529/jeet.34.16.21. Accessed 20 Aug. 2023.

16. Babu, Dr P. Sankar, et al. "Intelligents Traffic Light Controller for Ambulance." Journal of Image Processing and Intelligent Remote Sensing(JIPIRS) ISSN 2815-0953, vol. 3, no. 04, 19 July 2023, pp. 19–26, journal.hmjournals.com/index.php/JIPIRS/article/view/2425/2316, https://doi.org/10.55529/jipirs.34.19.26. Accessed 24 Aug. 2023.

17. S. Maddilety, et al. "Grid Synchronization Failure Detection on Sensing the Frequency and Voltage beyond the Ranges." Journal of Energy Engineering and Thermodynamics, no. 35, 4 Aug. 2023,

pp. 1–7, https://doi.org/10.55529/jeet.35.1.7. Accessed 2 May 2024.

18. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21, https://doi.org/10.55529/jeet.34.16.21. Accessed 20 Aug. 2023