# ENHANCING EFFICIENCY AND SECURITY: A G-CLOUD-BASED FRAMEWORK FOR GOVERNMENT HEALTHCARE SERVICES

**[1]K. Madhavi,[2]I. Siva Lakshmi,[3]T. Rajesh,[4]Venkata Siva Koti Rambabu Vudatha**

[1,2,3]Assistant Professor, Department of CSE, G V R & S College of Engineering &Technology, Guntur, AP

[4]Student, Department of CSE, G V R & S College of Engineering & Technology, Guntur,AP

**Abstract:** With the advancement of technology and the confinements of the good old medical services framework, an unplanned structure for social insurance is needed. We've witnessed a growing interest in and preference for cloud-based software development in the human services sector to manage and meet existing and future demands in social insurance administrations. We propose a cloud-based framework for medical services that is adaptable, safe, efficient, practical, and protected. For the administration EHR framework, we've presented a safe and effective structure in which fine-grained access control is commonly controlled by multi-authority ciphertext property-based encryption (CP-ABE), close by many levels of information structure to permit access control arrangements. E-government distributed computing is a major advantage for Saudi Arabia's top officials, who will be able to grow up their social insurance sector through the proposed framework.

**Index Terms:** Cloud Computing, Electronic Health Record, Security, Attribute-based Encryption, Ciphertext policy, Identity Proofing, Authentication, Authorization

## 1. INTRODUCTION

It's challenging to provide comprehensive care that includes illness prevention as well as treatment in most Arab countries' healthcare because of a lack of optimal utilisation of available human and material resources. The World Health Organization has reported the frequency of various diseases in Arab countries, including diabetes, hepatitis, and parasitic diseases including histoplasmosis and malaria (WHO). In many cases, recognising health problems early enough allows patients to avoid or reduce the severity of their symptoms. These difficulties include planning, operational, and technical considerations, all of which have an impact. If these difficulties can be overcome, we should expect a significant improvement in health care. It is difficult for medical institutions to keep comprehensive control of their operations and resources since the most cutting-edge software for managing all elements of technical and administrative healthcare is inadequate and underutilised. The performance of these high-end computers does not depend on the storage or software used to store their data. These systems' effectiveness hinges on their capacity to be accepted by a wide range of users, including healthcare practitioners, such as doctors, nurses, and technicians, as well as administrators, who have diverse information needs and priorities.

## 2. LITERATURE SURVEY

### 2.1 Q. Huang, Y. Yang, and M. Shen, ‘‘Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing,’’ Future Gener. Comput. Syst., vol. 72, pp. 239–249, Jul. 2017.

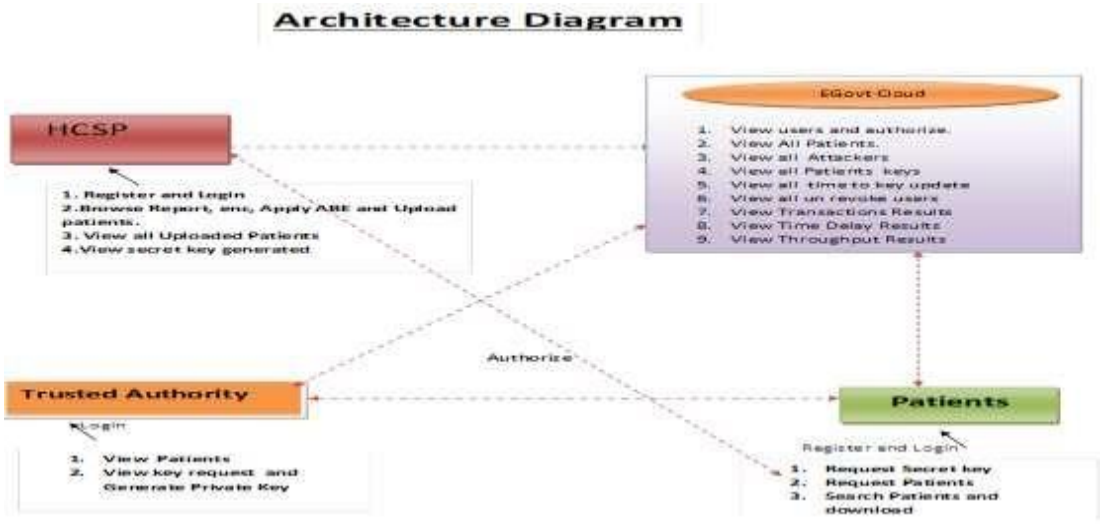
With the expanding pattern of redistributing information to the cloud for productive information stockpiling, secure information coordinated effort administration including information peruse and write in distributed computing is direly required. Nonetheless, it presents numerous new difficulties toward information security. The key issue is the best approach to bear the cost of secure compose procedure on ciphertext cooperatively, and along these lines different issues remember trouble for key administration and substantial calculation overhead on client since helpful clients may peruse and compose information utilizing any gadget. during this paper, we propose a protected and effective information coordinated effort conspire, during which fine-grained get to control of ciphertext and secure information composing activity are frequently managed bolstered quality-based encryption (ABE) and characteristic based mark (ABS) individually. to lighten the property authority from overwhelming key administration trouble, our plan utilizes a full appointment system bolstered progressive characteristic based encryption (HABE). Further, we additionally propose a fractional unscrambling and marking development by designating the majority of the calculation overhead on client to cloud specialist co-op. the wellbeing and execution examination show that our plan is secure and proficient.

**2.2 C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, ‘‘Secure integration of IoT and cloud computing,’’ Future Gener. Comput. Syst., vol. 78, pp. 964–975, Jan. 2018.**

Cloud Computing might be another innovation which alludes to a foundation where the two-information stockpiling and preparing work outside of the cell phone. Another ongoing innovation is the Internet of Things. Web of Things might be another innovation which is developing quickly inside the field of media communications. All the more explicitly, IoT related with remote media communications. The most objective of the communication and participation among things and articles which sent through the remote systems is to fulfill the objective set to them as a consolidated element. also , there's a fast improvement of the two innovations, Cloud Computing and Internet of Things, respect the segment of remote correspondences. During this paper, we present a study of IoT and Cloud Computing with consideration on the wellbeing issues with the two innovations. In particular, we join the 2 previously mentioned advancements (i.e Cloud Computing and IoT) in order to take a gander at the regular highlights, thus as to get the benefits of their combination. Finishing up, we present the commitment of Cloud Computing to the IoT innovation. Along these lines, it shows how the Cloud Computing innovation improves the capacity of the IoT. At long last, we review the security difficulties of the blending of IoT and Cloud Computing.

## 3. PROPOSED WORK

- Provides a flexible, secure, cost-effective, and privacy- preserved G-cloud-based framework for government healthcare services by: o Applying, using, and modifying the most recent encryption and decryption mechanisms suited for cloud-based EHR systems.
- The proposed scheme does not use the standard encryption system, which is not suited to the cloud environment. o Achieving scalability of computing resources that can be expanded and controlled according to the required health services. The EHR is able to support massive data exchanges. o Providing an effective solution for decision makers in the government health sector to adopt cloud- based healthcare systems, especially in developing countries. Providing a better authentication multifactor applicant authentication in cooperation with two trusted authorities.
- Different domains of attributes are managed by different attribute authorities, which operate independently from each other and controlled by the central trusted authority.
- Security analysis has been conducted according to major security requirements in cloud environments.



### 3.1 IMPLEMENTATION

- **HCSP**

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the patients details and will do the following operations like Upload Patient Details,View All My Uploaded Patients,View Public Keys,View Transaction Details.

- **Patients**

In this module, user logs in by using his/her user name and password. After Login user requests search control to cloud and will Search for Patients based on the index keyword with the Score of the searched Patient and downloads the Patient. User can view the search of the Patients and also do some operations like Search, Request Key, Request File, and View Keys

- **EGovt Cloud Server**

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data Patients and store them in the cloud for sharing with Remote User and will do the following operations like View HSPs and Patients, View Patient Details, View Attackers,View Patient Keys,Un Revoke User ,View Transaction ,View Transactions Results ,View Time Delay Results ,View Throughput Results

- **Trusted Authority**

In this module, TA logs in by using his/her user name and password. After Login he will do some operations like View all Patients, Generate Public Key Requests, key generation

## 4. RESULTS AND DISCUSSIONS

**Fig 4.1 Home Page**

**Fig 4.2 Outsourcing Data securely**

**Fig 4.3 Uploaded File Keys Details**

## 5. CONCLUSION

In this paper, we proposed a secure cloud-based EHR frame- work that guarantees the security and privacy of medical data stored in the cloud, relying on hierarchical multi-authority CP-ABE to enforce access control policies. The proposed framework provides a high level of integration, interoper- ability, and sharing of EHRs among healthcare providers, patients, and practitioners. In the framework, the attribute domain authority manages a different attribute domain and operates independently. In addition, no computational over- head is completed by the government authority, and multi- factor applicant authentication have been identified and proofed. The proposed scheme can be adopted by any government that has a cloud computing infrastructure and provides treat- ment services to the majority of citizen patients. Future work includes implementing and evaluating the proposed scheme in a real-world environment.

## REFERENCES

[1] M. Masrom and A. Rahimli, ‘‘A review of cloud computing technology solution for healthcare system,’’ *Res. J. Appl. Sci., Eng. Technol.*, vol. 8, no. 20, pp. 2150–2155, 2014.

[2] A. Hucíková and A. Babic, ‘‘Cloud Computing in Healthcare: A Space of Opportunities and Challenges,’’ *Transforming Healthcare Internet Things*, vol. 221, p. 122, 2016.

[3] H. Yang and M. Tate, ‘‘A descriptive literature review and classification of cloud computing research,’’ *CAIS*, vol. 31, Apr. 2012, Art. no. 2.

[4] D. Zissis and D. Lekkas, ‘‘Addressing cloud computing security issues,’’*Future Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.

[5] V. K. Nigam and S. Bhatia, ‘‘Impact of cloud computing on health care,’’*Int. Res. J. Eng. Technol.*, vol. 3, no. 5, pp. 1–7, 2016.

[6] *How to Improve Healthcare with Cloud Computing*, Hitachi Data Systems, Santa Clara, CA, USA, 2012.

[7] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, ‘‘Security challenges in healthcare cloud computing: A systematic review,’’ *Global J. Health Sci.*, vol. 9, no. 3, p. 157, 2016.

[8] D. Sun, G. Chang, L. Sun, and X. Wang, ‘‘Surveying and analyzing secu- rity, privacy and trust issues in cloud computing environments,’’ *Procedia Eng.*, vol. 15, pp. 2852–2856, Jan. 2011.

[9] N. Khan and A. Al-Yasiri, ‘‘Identifying cloud security threats to strengthen cloud computing adoption framework,’’ *Procedia Comput. Sci.*, vol. 94, pp. 485–490, Jan. 2016.

[10] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, ‘‘Security issues for cloud computing,’’ *Optimizing Inf.Security Advancing Privacy Assurance: New Technologies: New technol.*, vol. 150, 2012).

[11] V. K. Omachonu and G. N. Einspruch, ‘‘Innovation in healthcare delivery systems: A conceptual framework,’’ *Innov. J., Public Sector Innov. J.*, vol. 15, no. 1, pp. 1–20, 2010.

[12] B. E. Reddy, T. V. S. Kumar, and G. Ramu, ‘‘An efficient cloudframework for health care monitoring system,’’ in *Proc. Int. Symp. Cloud Services Comput.*, 2012, pp. 113–117.

[13] M. Parekh and B. Saleena, ‘‘Designing a cloud based framework for health- care system and applying clustering techniques for region wise diagnosis,’’ *Procedia Comput. Sci.*, vol. 50, pp. 537–542, Jan. 2015.