# A Multi-Authority Cipher Text Attribute-Based Encryption (CP-ABE) for G2C

[1]Ch.Ramya, [2]K.V.V.L.Madhuri
[1]Final year student, M.SC(CS),Dept. of Computer Science, Ideal College of Arts & Sciences, Kakinada,AP,India
[2]Assistant professor, Dept. of Computer Science, Ideal College of Arts & Sciences, Kakinada,AP,India

**ABSTRACT:**
We propose an adaptable, secure, cost savvy, and protection preserved cloud-based system for the healthcare condition. We propose a safe and proficient structure for the administration EHR framework, in which fine-grained get to control can be managed dependent on multi-authority ciphertext attribute based encryption (CP-ABE), together with a progressive structure, to uphold get to control strategies. The proposed system will permit chiefs in the Kingdom of Saudi Arabia to build up the social insurance segment and to profit by the current e-government cloud computing stage Yasser, which is liable for conveying shared services through a profoundly proficient, dependable, and safe condition. This system means to give health services and offices from the government to citizens (G2C).

**KEYWORDS**: Identity Proofing, Authentication, Authorization

## 1] INTRODUCTION:

An average wonder in social protection in most Arab countries is the absence of ideal use of human and material resources available to give composed therapeutic administrations to thwart ailments and treat sicknesses after they occur. Estimations exhibit that Arab countries experience the evil impacts of high paces of clinical issues, for instance, diabetes, liver ailment, and parasitic diseases, for instance, histosomiasis and wilderness fever. These clinical issues could be hindered before they occur or their complexities prevented by early acknowledgment. This is a direct result of a mix of parts: orchestrating, operational, and specific. If we had the choice to vanquish them, this would incite colossal progression in the level of restorative administrations.

Revised Manuscript received on April 26th , 2020
*Corresponding Author
Ch. Ramya
mail id- chramya1987@gmail.com

Also, there is a deficiency and nonattendance of open facility information frameworks, which is unquestionably the most dynamic programming that really serves all specific and legitimate therapeutic administrations works out, ensuring that the clinical association has full control over the aggregate of its activities and resources. The accomplishments of these moved frameworks don't depend upon the particular decision of apparatus and programming for limit. Or on the other hand perhaps, their success depends upon their sensibility for different customers—from social protection providers, for instance, pros, orderlies, experts, and even administrators—where the vision and requirements of all of these classes differentiate, and their information needs vary, as do the benefits of all of these frameworks.

## 2] LITERATURE SURVEY:

Reddy, B. Eswara, TV Suresh Kumar, and GandikotaRamu [11] clarified that Telemedicine is a promising advancement which joins media transmission and Information Technology for social protection the board. Telemedicine gives quality restorative administrations paying little mind to money related and land impediments. It conveys social insurance administrations benefits between remote patients and pros. There is a huge enthusiasm for robotizing the patient's data gathering, building it to get to constantly by achieving steadfast quality. With the happening to getting omnipresence in appropriated processing, the way wherein data is shared and exchanged social protection frameworks is changed. It gives leasing model, versatility and data get to capacity without geographical limitations. In this paper, we base on the structure of a Cloud structure for Health Monitoring System (CHMS). It assembles patients wellbeing data and circulates them to a Cloud information store. Yang, Haibo, and Mary Tate [2] proposed a sheltered and versatile structure for Electronic Health Records EHR data sharing which joins Identity-based Encryption and Attribute-based Encryption together to maintain get the chance to control techniques. Through this framework a fine-grained get the opportunity to control plot on EHR can be maintained and adaptable access between

different fogs is enabled. We in like manner propose a novel structure to address the issue of unseemly data get to realized by a customer with various occupations and access rights to an EHR.

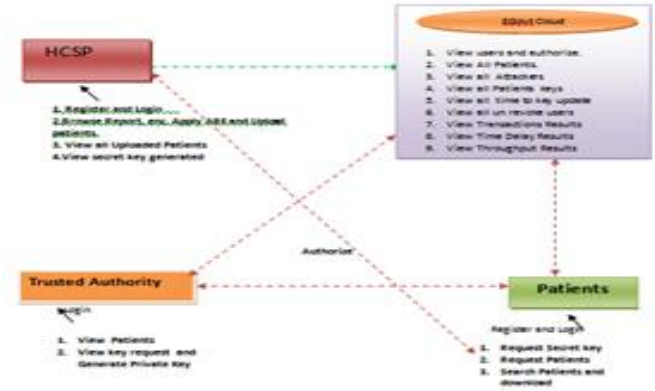
3] PROBLEM DEFINTION:

In 2010, Wang et al. [30] proposed a Hierarchal trademark based encryption (HABE) plan by uniting the dynamic character based encryption system and the ciphertext-course of action property based encryption (CP-ABE) structure. , and subsequently making a presentation expressivity tradeoff, finally applying middle person re-encryption and listless re-encryption to their arrangement. In 2007, Bethencourt et al. [21] Ciphertext-procedure property based encryption (CP-ABE), as one of the most reassuring encryption frameworks in this field, allows the encryption of data by deciding a passage control approach over attributes, so only customers with a great deal of characteristics satisfying this game plan can unscramble the relating data.

4] PROPOSED APPROACH:

Gives a versatile, secure, monetarily adroit, and protection saved G-cloud-based structure for government social protection benefits by: o Applying, using, and adjusting the most recent encryption and deciphering parts fitting for cloud-based EHR frameworks. The proposed plot doesn't use the standard encryption structure, which isn't fit to the cloud condition. o Achieving flexibility of handling resources that can be expanded and constrained by the fundamental healthservices. The EHR can reinforce huge data exchanges. o Providing an amazing response for pioneers in the organization wellbeing section to grasp cloud-based restorative administrations frameworks, especially in making countries. Giving an unrivaled approval multifaceted competitor confirmation in investment with two trusted in experts.

**5] SYSTEM ARCHITECTURE:**




**6**] PROPOSED METHODOLOGY:

6.1] HCSP

The information proprietor transfers their information in the cloud server. For the security reason the information proprietor scrambles the patients subtleties and will do the accompanying tasks like Upload Patient Details,View All My Uploaded Patients,View Public Keys,View Transaction Details

6.2] Patients

Client signs in by utilizing his/her client name and secret phrase. After Login client demands search control to cloud and will Search for Patients dependent on the list catchphrase with the Score of the looked through Patient and downloads the Patient. Client can see the pursuit of the Patients and furthermore do a few tasks like Search, Request Key, Request File, and View Keys

6.3] EGovt Cloud Server

The cloud server deals with a cloud to give information stockpiling administration. Information proprietors encode their information Patients and store them in the cloud for imparting to Remote User and will do the accompanying activities 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

6.4] Trusted Authority

TA signs in by utilizing his/her client name and secret key. After Login he will do a few tasks like View all Patients, Generate Public Key Requests, key age.

7] ALGORITHM:

Ciphertext Attribute-Based Encryption (CP-ABE)

Stage 1: Create Attribute Authority (PK, AA). Furthermore, accepts AA as info it is executed by the GA(government authority)

Stage 2: The Ministry of Health classifies the AAs as indicated by their functionalities and afterward appoints the characteristics for clients of these functionalities.

Step 3:AttributeKeyGenerator (PK, SKAid, Sid). This calculation is executed by the Aid space authority. It takes as info the PK and the area

authority's mystery key, SKAid, and the arrangement of properties, Sid. It yields the property mystery keys for the client SKUj.

Stage 4: The encode calculation takes as info the PK, a message (M), an entrance strategy (P), and the arrangement of open client keys (PKUs) relating to all the qualities in P. It yields the ciphertext message CT.

Stage 5: The unscramble calculation takes as information the PK, a ciphertext message CT, a similar access P utilized in encryption, the mystery client key, SKUj, and the arrangement of mystery property keys, SKA.

## 8] RESULTS:

| Scheme | ABE [20] | HABE [30] | MA-ABE [38] | FHTR PC ABE [25] | PC-ABE [39] | KP-ABE [39] | Symmetric/ public key | Proposed Framework |
|---|---|---|---|---|---|---|---|---|
| Multiple Authentication | No | No | No | No | No | No | No | Yes |
| Cloud Based | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| Fine-grained access control | No | No | No | Yes | Yes | Yes | No | Yes |
| Data privacy | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| Efficiency | Average | Average | Average | High | High | Average | Low | High |
| Scalability | No | No | No | Yes | Yes | No | No | Yes |
| Data Confidentiality | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| collusion resistant | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| Multi/Single AA | Single | Single | Multi | Single | Single | Single | Single | Multi |

Comparing the proposed framework with the existing schemes

## 9] CONCLUSION:

We proposed a safe cloud-based EHR system that ensures the security and protection of clinical information put away in the cloud, depending on hierarchical multi-authority CP-ABE to implement get to control approaches. The proposed structure gives an elevated level of coordination, interoperability, and sharing of EHRs among healthcare suppliers, patients, and specialists. In the system, the quality space authority deals with an alternate characteristic area and works autonomously. Also, no computational overhead is finished by the administration authority, and multifaceted candidate verification have been recognized and proofed.

## 10] EXTENSION WORK:

Future work includes implementing and evaluating the proposed scheme in a real-world environment.

## 11] REFERENCES:

[1] Masrom, Maslin, and AilarRahimli. "A Review of Cloud Computing Technology Solution for Healthcare System." Research Journal of Applied Sciences, Engineering and Technology 8, no. 20 (2014): 2150–2155.

[2] HUCÍKOVÁ, Anežka, and AnkicaBabic. "Cloud Computing in Healthcare: A Space of Opportunities and Challenges." Transforming Healthcare with the Internet of Things (2016): 122.

[3] Yang, Haibo, and Mary Tate. "A descriptive literature review and classification of cloud computing research." CAIS 31 (2012): 2.

[4] Zissis, Dimitrios, and DimitriosLekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no. 3 (2012): 583–592.

[5] Nigam, Vaibhav Kamal, and Shubham Bhatia. "Impact of Cloud Computing on Health Care." (2016).

[6] Mehraeen, Esmaeil, MarjanGhazisaeedi, JebraeilFarzi, and SagharMirshekari. "Security Challenges in Healthcare Cloud computing: A Systematic Review." Global Journal of Health Science 9, no. 3 (2016): 157.

[7] Sun, Dawei, Guiran Chang, Lina Sun, and Xingwei Wang. "Surveying and analyzing security, privacy and trust issues in cloud computing environments." Procedia Engineering 15 (2011): 2852–2856.

[8] Khan, Nabeel, and Adil Al-Yasiri. "Identifying cloud security threats to strengthen cloud computing adoption framework." Procedia Computer Science 94 (2016): 485–490.

[9] Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies 150 (2012).

[10] Omachonu, Vincent K., and Norman G. Einspruch. "Innovation in healthcare delivery systems: a conceptual framework." The Innovation Journal: The Public Sector Innovation Journal 15, no. 1 (2010): 1–20.

[11] Reddy, B. Eswara, TV Suresh Kumar, and GandikotaRamu. "An efficient cloud framework for health care monitoring system." In Cloud and Services Computing (ISCOS), 2012 International Symposium on, pp. 113-117. IEEE, 2012.

[12 Parekh, Maulik, and B. Saleena. "Designing a cloud based framework for healthcare system and applying clustering techniques for region wise diagnosis." Procedia Computer Science 50 (2015): 537–542.

[13] Botta, Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. "Integration of cloud computing and internet of things: a survey." Future Generation Computer Systems 56 (2016): 684–700

[14] Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. "Secure integration of IoT and cloud computing." Future Generation Computer Systems 78,(2018):964–975.

**Ch.Ramya** is a student of Ideal College of Art & Science, Kakinada Presently she is pursuing his M.Sc(Computer Science) from this college and she received his BSc from A.S.D Government Degree CollegeKakinada in the year 2018. His areas of interest includes Computer Networks and Object Oriented Programming languages, all current trends and techniques in Computer Science.

**Ms.K.V.V.L.Madhuri** is presently working as Assistant Professor in P.G Department of Computer Science, Ideal College of Arts& Sciences, Kakinada. She obtained her M.Sc in Computer Science from Andhra University. She has 2+ years of teaching experience at Post Graduate Level. Her areas of interest include Software Engineering, Data Structures, Database Management Systems, Computer Organization, Computer Networks.