A Novel Framework With High Level Of Integration, Interoperability, Among Healthcare Departments

[1]Ms.Mangalagiri Hema, [2]Ms.Konapalli Venkata Durga Devi
[1]M.Tech-CSE (Pursuing) Kakinada Institute of Engineering & Technology For Women, Korangi,
[2]Assistant Professor, Department of CSE, Kakinada Institute of Engineering & Technology For Women, Korangi.

ABSTRACT:
We propose a safe and effective system for the government EHR framework, in which fine-grained access control can be managed dependent on multi-authority ciphertext-attribute-based- encryption (CP-ABE), along with a hierarchical structure, to implement access control strategies. The projected system will permit chiefs in the Kingdom of Saudi Arabia to build up the healthcare sector and to profit by the current e-government cloud computing stage, which is answerable for conveying shared admin through a profoundly proficient, dependable, and safe condition. The projected plot is appropriate for G-based cloud EHR frameworks and gets advantages from the facilities and the foundation gave by the legislature. We accept that our system contribute in utilizing a changed variant of the PC-ABE scheme with multi-attribute and multi-factor proofing authentication.

KEYWORDS: Ciphertext, cloud, Authentication

1] INTRODUCTION:

The fast move to the cloud and its utilization in healthcare systems has raised worries about essential issues of protection and data security. The selection of the cloud in IT expands the concentration and worry of human services suppliers on clinical and tolerant related administrations and lessens consideration on foundation the board [6]. The sharing of individual and health data over the Internet and different servers outside the sheltered condition of the human services establishment has prompted various issues identified with protection, security, access, and consistence issues.

The accomplishments of these propelled frameworks don't rely upon the specific determination of hardware and software for storage. Or maybe, their prosperity relies upon their reasonableness for various clients from healthcare services suppliers, for example, specialists, attendants, experts, and even managers where the vision and needs of every one of these classes contrast, and their data needs change, as do the advantages of every one of these systems[2,14].

2] LITERATURE SURVEY:

Masrom, et al[1] described CP-ABE is a promising cryptographic solution with this issue. It authorize information owners to define their own access policies over client properties and implement the policies on the information t o be distributed. This adequately wipes out the need to depend on the information storage server for preventing unapproved information access and honesty. The presentation and security investigations show that the projected plot is proficient to safely deal with the information stored in the main storage servers

Yang et al,[3] With the progression of innovation and the confinements of the regular healthcare framework, an improvised structure for healthcare framework is required. This paper presents another cloud based skeleton which relates key portions of any healthcare system which show restraint, specialist, side effect and sickness. The paper on a very basic level focuses on how these parts are between related and how we can gather reasonable information from them. As a usage, it shows the fundamental social insurance analyser interface which takes data as input and mines the data by utilizing a portion of the information mining methods like bunching. It is helpful for government associations which point at exploring therapeutic issues and to improve health conditions of India.

3] PROBLEM DEFINTION:

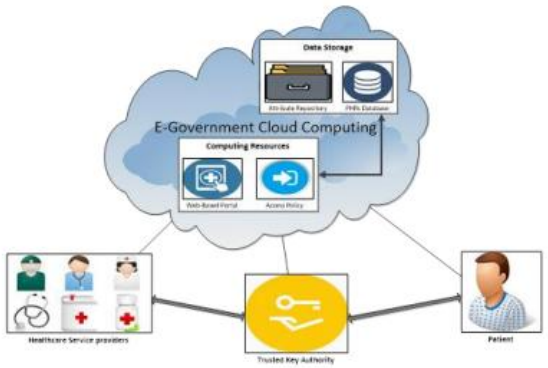
In 2012, Zisis et al[4] proposed an expressive decentralizing KP-ABE scheme. The ciphertext size doesn't depend on the quantity of property utilized in ciphertext. Client's keys are appended with get to structures and ciphertext is related with characteristics. A client can unscramble, if ciphertext's traits is the approved arrangement of the entrance structure.

In 2016, Mehreen et al[7]. CP-ABE, as one of the most encouraging encryption frameworks in this field, permits the encryption of information by indicating an access control policy over attributes, so just clients with a lot of properties fulfilling this policy can decrypt the corresponding data.

4] PROPOSED APPROACH:

A cloud-based theoretical formation has been created for the step up of electronic health services in Saudi Arabia. The projected structure will permit leaders to build up the health zone and to profit by the services gave by different parts in the realm, for instance, the electronic services framework called Absher, which is utilized by the Ministry of the Interior to guarantee the individual personality of the recipients and the e-government cloud stage, which is liable for delivering shared services through an highly productive, dependable, and safe condition.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

HCSP:

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

PATIENTS:

Client signs in by utilizing his/her client name and secret password. After Login client requests 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

EGOVT CLOUD SERVER:

The e-government cloud-based EHR is the base of our planned work. In the Kingdom of Saudi Arabia, the e-government plan (Yesser) has been built up, and one of its drives and items is government cloud computing. This Gov cloud gives proficient, secure, dependable structure, stage, softwares, all as services.

HEALTHCARE PROVIDERS:

Healthcare suppliers are people who give healthcare services of various sorts in a composed way to all individuals from a network. The medicinal services suppliers could incorporate the accompanying individuals: health practitioners and specialists, physicians, nurses, pharmacists, surgeons, medical technicians, laboratory workers, and other employees.

7] ALGORITHM:

CP-ABE:

Stage 1: Build Attribute Authority (PK, AA). And accepts AA as information it is execute by the GA(government authority)

Stage 2: The department of Health sorts the AAs as per their functionalities and afterward assigns out the attributes for clients of these functionalities.

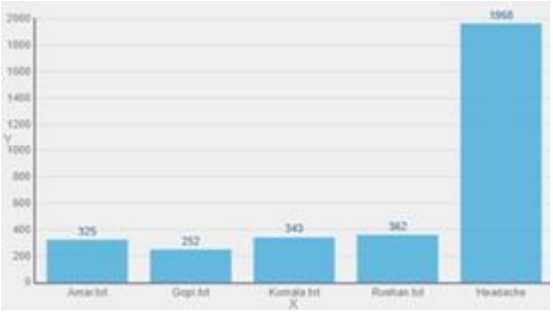
Stage 3: Attribute KeyGenerator (PK, SKAid, Sid). This algorithm is performed by the Aid domain authority. It takes as input the PK and the area authority's secrecy key, SKAid, and the arrangement of traits, Sid. It yields the attribute secret keys for the client SKUj.

Stage 4: The encode algorithm takes as information the PK, a message (M), an access policy (P), and the arrangement of public user keys (PKUs) comparing to all the properties in P. It yields the ciphertext message CT.

Stage 5: The decrypt algorithm takes as info the PK, a ciphertext message CT, a similar access P use in encryption, the secret client key, SKUj, and the array of secret attribute keys, SKA.

8] RESULTS:

Attacked Files and Revoked Users



Time delay details in EGovt cloud

9] CONCLUSION:

We proposed a protected cloud-based EHR system that ensures the security and security of clinical information put away in the cloud, depending on various leveled multi-authority CP-ABE to uphold access control approaches. The proposed structure gives an elevated level of reconciliation, interoperability, and sharing of EHRs among healthcare suppliers, patients, and professionals.

10] REFERENCES:

[1] Masrom, Maslin, and Ailar Rahimli. "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 Ankica Babic. "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 Dimitrios Lekkas. "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).

[7] Mehraeen, Esmaeil, Marjan Ghazisaeedi, Jebraeil Farzi, and Saghar Mirshekari. "Security Challenges in Healthcare Cloud computing: A Systematic Review." Global Journal of Health Science 9, no. 3 (2016): 157.

[8] 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.

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

[10] 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).

[11] 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.

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

[13] 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.

[14] 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

[15] 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.

PROFILES:

Ms. Mangalagiri Hema is a student of Kakinada Institute of Engineering & Technology For Women, Korangi. Presently she is pursuing her M.Tech [Computer Science and Engineering] from this college and she received her B.Tech from Aditya College of Engineering and Technology, affiliated to JNT University, Kakinada in the year 2018. Her area of interest includes Cloud Computing and Web Technologies, all current trends and techniques in Computer Science.

Ms.Konapalli Venkata Durga Devi, Assistant Professor, Department of CSE, Kakinada Institute of Engineering & Technology for Women, Korangi.