https://doi.org/ 10.33472/AFJBS.6.10.2024.629-635

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

A Survey on Dynamic ABE Scheme with Block Chain Based Authorities for Medical on Demand

[1] Supriya Reddy Yellatooru ,[2] Thota sai lalith Prasad , [3] D.shivasai

[1]Assistant Professor in Department of CSE G .Pulla Reddy Engineering College, Kurnool

[1] supriyareddy.cse@gprec.ac.in

[2]Assistant Professor in Department of CSE Teegala Krishna Reddy Engineering College

[3]Assistant Professor in Department of AIM Teegala Krishna Reddy Engineering College

,[2] sailalith15@gmail.com ,[3] saishiva538@gmail.com

Article History
Volume 6,Issue 10, Feb 2024
Received:17 Mar 2024
Accepted : 01 May 2024

doi: 10.33472/AFJBS.6.10.2024.629-635

ABSTRACT- As the cloud computing technology is increasing its boom, its importance in the medical services is also increased. We propose, a security mechanism for the cloud to store all the data from the hospitals such as electronic health records (EHRs) with ABE scheme based on block chain technology. It offers the hospital authorities and the users the security to login and also store their private data. Attribute-based encryption (ABE) algorithm realizes flexible and fine-grained access control, a large number of patients subscribe or unsubscribe the different medical services frequently in the cloud, which takes a huge cost for membership management. In this paper, we will construct a dynamic key policy ABE scheme in the distributed telemedicine system with the keys sent to the users and the authorities. The user and the authority's credentials are not overlapped. They are stored within their boundaries with all the CP-ABE and the KP-ABE schemes. With the Block chain technology, the Personal Healthcare Information stored in public cloud is covered in integrity, which avoids the misdiagnosis coincidence from the wrong electronic fitness information distorted by a malicious user or authority from the internal cloud. Ultimately, we analyse the collusion assault in multiple authorities and formally show the safety of this protocol in a well-formed version.

Key terms: ABE scheme, Block Chain, CP-ABE, KP-ABE, EHRs

OVERVIEW

Mostly, this paper is investigating the dictator-following consensus problems with the dual-agent system with continuously monitoring the interaction constraints and have unreliable interaction environment. The two kinds of interaction schemes are event-trigger and self-trigger schemes and they have been well designed and efficiently performed in the attacks of Denial of Service. In these interaction schemes, synchronous and asynchronous types of controlling protocols have been deployed, which will guarantee the dual agents to effectively achieve the dictator-following consensus in an untrustworthy network type of environment. The self-Triggered scheme is further decreased the event detection cost, it also determines the next triggering by computing it.

EXISTING SYSTEM

In this we have a cloud service provider, in which it connects the patient with the medical staff who are in the different position with the convenience and also the fidelity. In the meanwhile, the healthcare data on the public clouds brings extra challenges on the security. The Attribute Based Encryption algorithm realizes flexible and fine grain access control mechanism, which have large number of patients who are subscribed and Also unsubscribed from the different medical services who are present in the cloud, it takes huge cost for the membership

LIMITATIONS

The requirements of the medical resources increases drastically in this health care system. The subscribed patients who are living in the rural areas, in which the traffic flow is inconvenient, and are more in lack of mobility and as well as accessing the authority to high quality health care and especially for the aged and also the disabled ones.

PROPOSED SYSTEM

In this proposed system, we are proposing an ABE algorithm with an authentication and authorization schemes with high flexibility and efficiency for the medical on demand (MoD) services of telemedicine. The patients who wants to order service, they must have to enrol or subscribe for the telemedicine. Whenever the patient, uses an alter option in the service then it must not require any update in the parameters and the statuses are remained unaffected. We propose a key policy ABE scheme in which the telemedicine system is distributed and also it aims to update the patient's keys uniquely and the dual authorities that should manage this system together, that is more similar to the real situation. We can use another technology like block chain with the database technologies for the storing the health care data in the public cloud in a protected manner in the integrity. By this we can avoid the misdiagnosis accidents data from the inaccurate information in the EHRs. Malicious users and also the attacks can be removed by the proposed system. The efficiency of the cloud storing can be evaluated to a maximum with the key based ABE scheme.

ADVANTAGES

The advantages of this proposed system is the rural area patients can also able to interact with the different areas dual agents, which will overcome the issues with the distance so that we can increase the medical on demand services in the rural areas and also saves the lives in critical and emergency situation in the rural areas.

METHODOLOGY:

The proposed scheme will effectively works on the privacy issues of the patients who are already subscribed for the medical on demand services through online. Block chain technology is used for the integrity and the data is stored in the chain of transactions in the cloud. Cloud is used to store the encrypted ehr for future use. After successful download of ehr the patient can get the key to decrypt the ehr.

The key policy based Attribute based encryption mechanism is used to encrypt the patient record with the unique patientid and the record is sent to the cloud with the help of block chain hashing technique. The patient whenever they want to know their respective ehr, then the key is used to decrypt the ehr, every patient will have a unique key.

The authority will be responsible for the uploading of the ehrs into the cloud. Whenever patient enquires for the ehr, the cloud will send the request access to the authority whenever the authority gives the response with the key then only the patient will get the download option for their respective ehr.

With this the integrity and the privacy information of the user is secured.

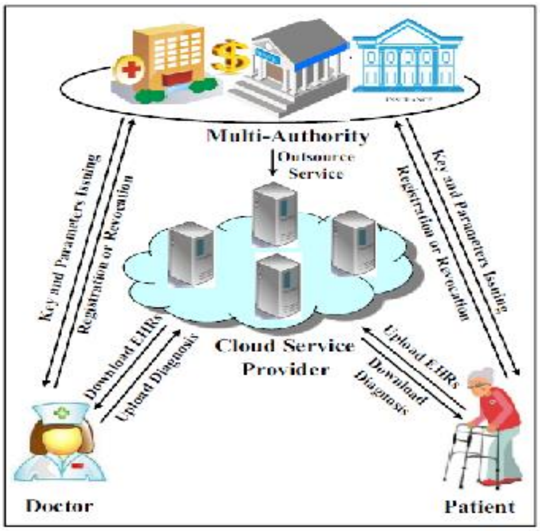

Fig1. Proposed method

The proposed methodology ABE scheme with multi-authority, we construct seven algorithms that are provided in detailed as follows.

Global Setup: This algorithm consists of three steps.

Step 1. Given the security parameter 1δ , the telemedicine system generates a bilinear mapping eˆ : G × G → GT with generators g, h of G, where G and GT are additive cyclic group and multiplicative cyclic group respectively whose orders are the same prime value p. Step 2. Generating two default patients with global identity {GID0,GID1}. Supposing that there is a strong collision resistant hash function H : {0, 1} ∗ → Z ∗ p , computing two default patients U = {u0 = H(GID0), u1 = H(GID1)}. Randomly choosing 2(|A˜|+1) elements{vi,j} ∀i∈U,j∈{1,2,...,|A˜|}, and {ti}∀i∈U in Z ∗ p , computing {Vj = (Y ∀i∈U vi,j)g} j∈{1,2,...,|A˜|}, {vi,j = Y k6=i,k∈U v −1 k,j + tivi,j} ∀i∈U,j∈{1,2,...,|A˜|}. Step 3. The public parameters are the tuple of params = (eˆ, G, GT , p, g, h, H,{Vj,{vi,j}∀i∈U } ∀j∈{1,2,...,|A˜|}, Ver), where Ver is a version number of these parameters.

Authority Setup: This algorithm consists of four steps.

Step 1. Generating N authorities A1, A2, · · · , AN . For each authority Aq, it manages its attribute set A˜ q = {˜aq,1, a˜q,2 . . . a˜q,nq }q∈[1,N] , and picks αq ∈ Z ∗ p randomly, computes wq = ˆe(g, g) αq . For each attribute a˜q,m ∈ A˜ q, where m ∈ [1, nq], selects γq,m ∈ Z ∗ p randomly and computes Tq,m = γq,mg, T 0 q,m = γq,mh. Step 2. Two authorities Aq and Al share a value sql ∈ Z ∗ p between themselves as a pseudorandom function (PRF) seed which is transmitted in the two-party key exchange channel secretly, and it can be found that sql = slq obviously.

Step 3. Aq and Al choose xq, xl ∈ Z ∗ p respectively, and take a secure key agreement protocol to define a PRF for two patients as PRFq,l(u{0,1}) = xqxl sql + u{0,1} h, where u{0,1} represents a hash value of GID0 or GID1. Step 4. Authority Aq outputs his public key as PKq = (wq,{Tq,m, T 0 q,m}m∈[1,nq]), while its private key is SKq = (αq, xq,{sql}l∈{1,2,...,N}\{q},{γq,m}m∈[1,nq]).

KeyGen: Based on the tuple of params, a new Patient i takes part in the telemedicine system. Let A be an access policy of Patient i, this algorithm returns a tuple of private keys that enables this new Patient i to obtain the cipertext CT only if the attribute of CT satisfies this access policy A. This algorithm consists of four steps. Step 1. The authority randomly picks (|A˜| + 1) elements {ti,{vi,j} ∀j∈{1,2,...,|A˜|}} in Z ∗ p . Step 2. Setting U = U ∪ {i}, authority Aq chooses rq ∈ Z ∗ p .

Step 3. Patient i interacts with every authority Aq in N − 1 times to achieve the anonymous key issuing. Then, it computes Dql = αqg + rqh + PRFql(i) for q > l, Dql = αqg + rqh − PRFql(i) for q < l, and Di = X (q,l)∈{1,2,...N}×({1,2,...N}\{q}) Dql = X N q=1 (N − 1)αqg + X N q=1 (N − 1)rqh,

{Vj = vi,jVj} ∀j∈{1,2,...,|A˜|}, {vi,j = Y k6=i,k∈U v −1 k,j + tivi,j} ∀j∈{1,2,...,|A˜|}, {vk,j = (vk,j − tk vk,j)v −1 i,j + tk vk,j} ∀k6=i,k∈U,j∈{1,2,...,|A˜|}. Step 4. Let A be an access policy over the set of attributes A˜. By using of the linear secret sharing scheme, we can obtain the share {βj} of the secret s ∈ Z ∗ p . It denotes the element corresponding to the share βj as a˜j ∈ A˜, where aj is the attribute underlying a˜j . Note that a˜j may be negated or non-negated attribute. For every j such that a˜j is non-negated attribute, D (1) i,j = {v −1 i,j βjαqg}q∈{1,2,...,N}, D (2) i,j = { v −1 i,j βjrq 1 + ti(Q i∈U vi,j) h}q∈{1,2,...,N}, D (3) i,j = {tiβjαqg}q∈{1,2,...,N}, D (4) j = {βjrqh}q∈{1,2,...,N} . For every j such that a˜j is negated attribute, D (5) i,j = { βj Pnq m=1 γq,m (Di)}q∈{1,2,...,N}, D (6) j = βj Pnq m=1 γq,m rqg. The private key of patient i consists of the above group elements that SKi = (D (1) i,j , D (2) i,j , D (3) i,j , D (4) j , D (5) i,j , D (6) j).

Revoke: This algorithm is aimed to revoke the private key of some registered patient u, the authority increases the version number Ver and updates {Vj,{vi,j}∀i∈U } ∀j∈{1,2,...,|A˜|} in params in the following, {Vj = v −1 u,j Vj} ∀j∈{1,2,...,|A˜|}, {vk,j = (vk,j − tk vk,j)vu,j + tk vk,j} ∀k6=u,k∈U,j∈{1,2,...,|A˜|}. Then, the authority deletes {vu,j} ∀j∈{1,2,...,|A˜|}. **Encrypt:** This algorithm takes (DEK, A˜, Params,s) as inputs, where A˜ is a set of attribute for the medical service, and encrypts this service under the DEK. A set of values {sj} j∈{1,2,...,|A˜|} is randomly selected, which satisfies the equation |A˜P | j=1 sjβj = s. Then, it outputs the ciphertext of the DEK as follows. CT = (A˜, c (0) = DEK · (Y N q=1 wq) s , {c (1) j = sjVj} j∈{1,2,...,|A˜|}, {c (2) j = sjg} j∈{1,2,...,|A˜|}, {c (3) j = Xnq m=1 sjTq,m} j∈{1,2,...,|A˜|},q∈{1,2,...,N} , {c (4) j = Xnq m=1 sjT 0 q,m} j∈{1,2,...,|A˜|},q∈{1,2,...,N} , Ver). **ReEncrypt:** This algorithm inputs the current parameters params, an exist ciphertext CT , and the corresponding s, it outputs the updated ciphertext CT ∗ which is accessed by replacing {c (1) j } ∀j∈{1,2,...,|A˜|} of CT with {c (1)∗ j = sjV ∗ j } ∀j∈{1,2,...,|A˜|}, where V ∗ j is the current public parameter.

Decrypt: Patient checks whether A(A˜) = TRUE holds or not. If not, outputs ⊥. Otherwise, executes the following. For each non-negated attribute a˜j ∈ A˜, patient computes Fj = Q N q=1 [eˆ(vi,j(D (1) i,j + D (2) i,j) − D (3) i,j , c (1) j)] Q N q=1 [eˆ(c (2) j , D (4) j)] = ˆe(g, g) sjβj PN q=1 αq . For each negated attribute a˜j ∈/ A˜, patient computes Fj = eˆ(D (5) i,j , c (3) j N−1) Q N q=1 [eˆ(c (4) j , D (6) j)] = ˆe(g, g) sjβj PN q=1 αq . Then, patient computes F = |A˜ Y | j=1 (Fj) = ˆe(g, g) s PN q=1 αq . Finally, patient obtains DEK that is uses to access the medical services by computing

DEK = c (0)/ F.

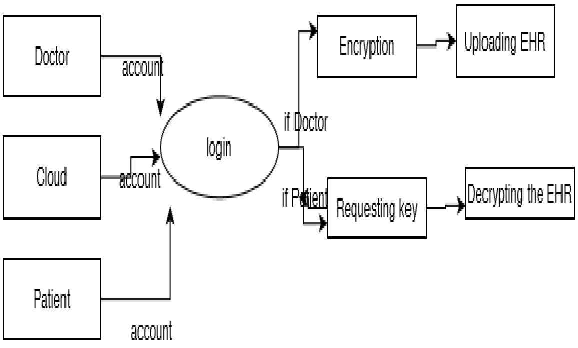

Figure 2: Flow

The above figure 2 represents the flow of the proposed system. The doctor can be an authority, cloud and the patients can login with their own credentials into the application. After entering the cloud will be able to see all the documents ehrs in its storage space. The doctor with his/her private key will encrypt the EHR and combining with the public key of the patient and performs encryption and sends it to the cloud.

The patient will request for the key from the authority to download the EHR from the cloud after successful download of the ehr, then the patient will decrypt with the private key and the key which he received from the authority.

DATASET:

The dataset used for the proposed method consists of the PatientId, Patient Name, Age, Height, Weight, Gender, Blood Group, BP, Body Type, Diseases, Haemoglobin, CBC, Cholesterol, Sugar, Handicapped, and Physically Challenged. All the details are filled with the authority like doctor or the hospital management. The other dataset used in the experiment consists of the seven attributes namely Patient ID, Patient Gender, Patient Date Of Birth, Patient Race, Patient Marital Status, Patient Language, Patient Population Percentage Below Poverty.

RESULTS:

After implementing the ABE scheme with block chain technology the percentage of patients in the rural areas have got more number of subscribers and the cloud storage for the patients have got more and more increased. This proposal can give the security for the privacy data of the patients. The below graph shows the increase in the percentage of the patients in every year.

The x-axis represents the year and y-axis represents the percentage of growth in the rural areas.

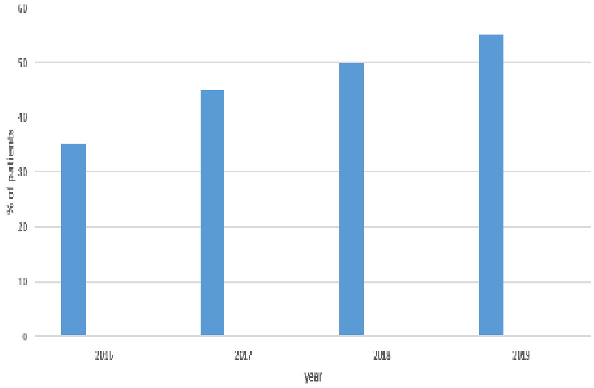

Fig.3 percent of rural patients

The computational time for encryption in the ABE scheme can be very much lesser and the notation for the computational cost is O(m_c X n_c).

The X-axis represents the number of attributes in the ciphertext and Y-Axis represents the computational time for encryption in milliseconds.

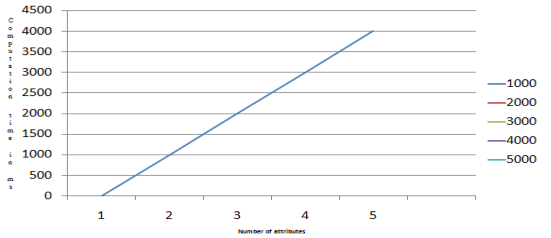

Figure 4: time for encryption

The computational time for decryption in the ABE scheme is very much lesser than that of other algorithms. The notation for this can be represented as O($m_U Xn$).

The x-axis represents the number of attributes in the user and the time of decryption on the y-axis.

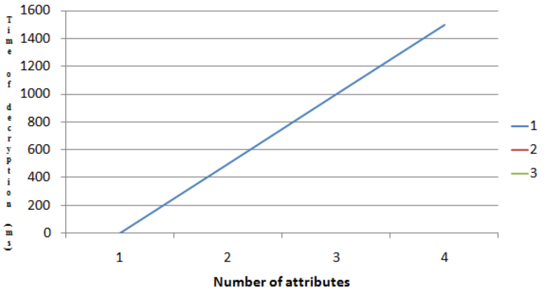

Figure 5: time for decyption

In the figure 6, It represents the marital status of the patients both male and female, who are going for the medical check-ups. The married patients are more often opting for the check-up clearly, we can see that in the figure.

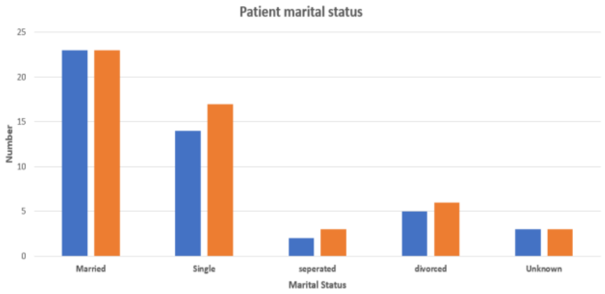

Figure 6: Marital status

In the Figure 7, It represents the year of birth of the patients of both male and female. In the bar graph, it is clearly represented that the patients belongs to the 1961-1980 are going for the medical check-ups.

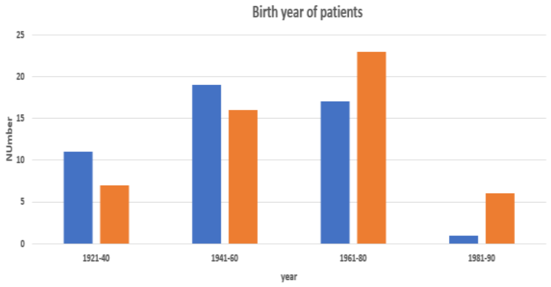

Figure 7: Year of birth

In the figure 8, It represent the various languages spoken by the patients. In the dataset, there are four languages that are Hindi, Marathi, Tamil, telugu.

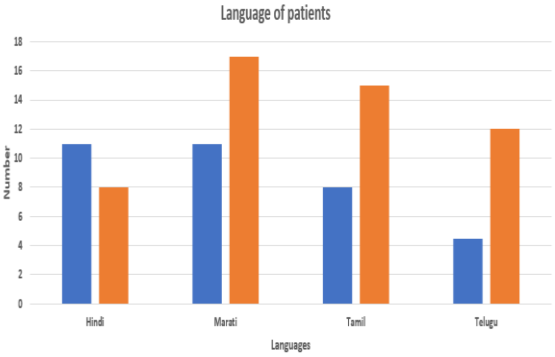

Figure 8: languages

In the Figure 9, It represents the race of Indian history, Like Caucasoid (white), Mongoloid (yellow),Negroid (black), Australoid.

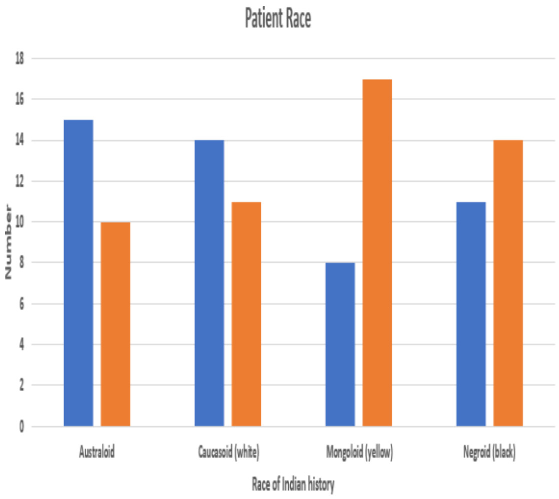

Figure 9: Patient Race

CONCLUSION:

The conclusion of this paper is that we can put forth an independent ABE scheme with the dual authorities, which is applied in the MoD service of telemedicine system. The patients will enrol in this service freely and can change the access policies on demand, in the unrelated patients they must have to renew their keys in registration and update before login and also ordering for a service. The block chain with ABE technology is used to chain all the patients' data to avoid tampering by the unauthorised user and authority.

FUTURE ENHANCEMENT:

The future enhancement of this can be a deduplication removal of the ehr from the cloud. For the removal of deduplication in the cloud we can use a policy based deduplication removal which will automatically removes the duplicate entries by the authorities. We can also keep away all the unauthorized authorities or the malicious users in the real time.

REFERENCES

[1] J. Matusitz and J. M. Breen, “Telemedicine : its effects on health communication," Health Commune., vol. 21, no. 1, pp. 73-83, 2007.

[2] World Health Organization, “Telemedicine : opportunities and developments in Member States: report on the second global survey on eHealth," WHO Global Observatory for eHealth, 2010. [Online].

[3] M. Berman and A. Fenaughty, “Technology and managed care: patient benefits of telemedicine in a rural health care network," Health Econ., vol. 14, no. 6, pp. 559-573, 2005.

[4] N. M. Hjelm, “Benefits and drawbacks of telemedicine," J. Telemed. Telecare, vol. 11, no. 2, pp. 60-70, 2005.

[5] A. Benharref and M. A. Serhani, “Novel cloud and SOA-based framework for e-health monitoring using wireless biosensors," IEEE J. Biomed. Health, vol. 18, no. 1, pp. 46-55, 2014.

[6] O. Ali, A. Shrestha, J. Soar and S. F. Wamba, “Cloud computing enabled healthcare opportunities, issues, and applications: a systematic review," Int. J. Inform. Manage., vol. 43, pp. 146-158, 2018.

[7] Y. Karaca, M. Moonis, Y. D. Zhang and C. Gezgez, “Mobile cloud computing based stroke healthcare system," Int. J. Inform. Manage., vol. 45, pp. 250-261, 201

[8] P. Mell and T. Grance, “The NIST definiti on of cloud computing," National Institute of Standards and Technology, NIST SP-800-145, 2011. [Online].

[9] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Kaz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, “A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50-58, 2010.

[10] M. Hamdaqa and L. Tahvildari, “Cloud computing uncovered: a research landscape," Adv. Comput., vol. 86, pp. 41-85, 2012.