A Cloud based Two Layered Access Control with Decentralized Anonymous Authentication in Health Care

R. Raghul Vaikundam
Department of Information Technology, Madras Institute of Technology, Chennai 60004,4 India
raghul.vaikundam3@gmail.com

D. Sangeetha
Assistant Professor
Department of Information Technology, Madras Institute of Technology, Chennai 600044, India
dsangeetha@mitindia.edu

V. Vaidehi
Senior Professor and Dean
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai 600127, India
vaidehi.vijayakumar@vit.ac.in

R. Srinandhakumar
Department of Information Technology, Madras Institute of Technology, Chennai 60004,4 India

V. Subhash Ignatius
Department of Information Technology, Madras Institute of Technology, Chennai 60004,4 India

Abstract*—Personal health record (PHR) is a patient-patronage paradigm for sharing health information which is outsourced to a third party server. There has been critical concern over privacy as the personal health information becomes vulnerable on exposure to unauthorized parties when ported onto cloud. In order to ensure privacy preservation, this paper proposes a Two Layered Access Control with Decentralized Anonymous Authentication (TLACDAA) which is sealed against replay and collusion attacks. To overcome these existing issues, the proposed TLACDAA uses Graph based Access Structure scheme which facilitates greater access control over health care data and protects patient sensitive information by encrypting it using Multiple Authority Cipher Text Policy Attribute Based Encryption with Advanced Encryption Standard. Moreover, the security of the proposed TLACDAA is enhanced by incorporating two levels of authentication. The first level of authentication is ensured with enhanced tokenization technique. The second level of authentication is done using MAC Anonymization technique which is known as Device Authentication. Thus the two layers of authentication mechanisms ensure an enhanced privacy for the patients in a health care cloud environment. Moreover, the cloud server restricts the access to those users with the similar set of attributes for preserving user's privacy by attribute based access control in TLACDAA. When the authentication schemes are implemented in a private cloud environment, it is observed that the proposed TLACDAA provides 17% improved efficiency when compared to the existing authentication and access control schemes.

Index Terms*—Personal Health Record, Attribute Based Encryption, Attribute Based Access Control, Anonymous Authentication, MAC Anonymization.

I. INTRODUCTION

A Personal Health Record [7], or PHR, is a health record in which patient maintains their health data. The PHR's intension is providing an accurate summary of an individual's medical history through online. It is an electronic application which is used by a diverse group of people to share their personal health data in a private environment. The source of data for PHR is either from health care providers like doctors, nurse or from the patient.

There are two types of users accessing the PHR namely Personal domain and Public domain users.

Personal domain users include patients, friends and relatives whereas Public domain users include researchers, Doctors and insurance agents. The existing PHR system, two layered access control system uses an attribute- based access control [3][8] mechanism is in which the system cannot be accessed by the user unless they have hold of keys for both security layers. The security of the system [15] is enhanced by this mechanism especially when many users share the same computer for web-based cloud services. Therefore, the proposed TLACDAA uses Two Layered Authentication with Graph Based Access Control (GBAC). By combining attributes together with predicates, access policy can be formulated using GBAC. The access policies can be formed using any type of attributes (role attributes or data attributes) and predicates (AND, OR).

When the PHR is outsourced to a third party server, privacy issue arises. In order to overcome the privacy issues in the cloud, Attribute Based Encryption (ABE)[3][8] is used. In Attribute Based Encryption (ABE)[3][8], the secret key of a user and the cipher text are dependent upon attributes. In ABE, the cipher text can be decrypted only when the attributes of all the user's key matches with the cipher text's attributes. When ABE is used in encrypting PHR, it is prone to collusion attacks [18]. Anonymous Authentication [AA] is the one in which without providing a user name and password, user can access any public content. The Milti-Authority Cipher-text Policy Attribute Based Encryption (MACPABE) helps in preserving the patient privacy by

978-1-7281-0353-2/18/$31.00 ©2018 IEEE

encrypting the patient's sensitive information. The two levels of authentication provides the greater level of data security for accessing the patient's record.

II. RELATED WORK

Personal Health Record (PHR) [2] [18] is an electronic record managed by patients in a centralized environment and it is stored on to the third party server which lead to privacy issues. In order to overcome this privacy issue, it is better to encrypt the PHR files before it is ported on to the cloud. Apart from privacy issue, there are some difficulty in scalable key management, access control and efficient user revocation. For a scalable key management, multiple security domains (public and personal domain) is introduced. The access privilege of role and data attributes are defined in public and personal domain respectively. Key distribution of public and private keys are made scalable which ensures improved privacy preservation. The patient privacy is enhanced by Hierarchical and Multi-Authority Attribute-Set Based Encryption (HM-ASBE) [3] [14]. In HM-ASBE scheme, compound attributes of ASBE with flexible fine grained access control are supported with on-demand and user revocation mechanisms.

Since cloud computing is beneficial when multiple users tries to share their data, effective anti-collusion data sharing scheme are developed. This group sharing scheme results in low maintenance and minimal management cost however there is some privacy concern and ineffective key management among group members. Due to poor key management, the scheme is susceptible to collusion attack. Therefore, anti-collusion data sharing scheme comprises of entities such as group manager, group member and cloud providers. Group member securely obtain their private keys from group manager and fine-grained access control is achieved. Any user in the group can access the resource however the revoked user cannot gain access to those resource once they are revoked. The scheme is resistant to collusion attack, which means the revoked user cannot get their original data when they request to the untrusted cloud.

The traditional authentication system is a password based authentication system. In Web based cloud computing service, when the spyware is inserted in the client browser, the password will be tracked by the spyware and traditional authentication can be broken easily. In order to overcome this problem, Two-Factor Authentication (2FA) access control system [1][8] was developed. The proposed 2FA is an attribute-based access control mechanism for web-based cloud computing services. In 2FA, the user can access the system with the hold of secret key of user and a lightweight security device.

A single point of trust in the Attribute based Signature (ABS) scheme will result in single point of failure. The existing system has hierarchical access policy which does not ensure fine grained access control. The existing system provides less privacy preservation since it does not follow any technique for anonymous authentication (tokenization). In the existing system, lightweight device is directly used as key without any hashing which results in user's identity. Hence, there is a need for an enhanced anonymous authentication mechanism which prevents the PHR setup from attacks and ensure privacy preservation.

III. PROPOSED TWO LAYERED ACCESS CONTROL WITH DECENTRALIZED ANONYMOUS AUTHENTICATION (TLACDAA)

A. Overview

The proposed TLACDAA is decentralized unlike existing access control mechanisms which throws a single point of failure with a central authority. A single point of trust in the existing Attribute based Signature (ABS) scheme is overcome by using multiple Attribute Authorities in the proposed TLACDAA. The proposed TLACDAA also supports the Create, Read, Update and Delete (CRUD) operations on the encrypted PHR data stored on the cloud for privacy concern. The proposed TLACDAA system introduces an enhanced authentication method that requires two layered access keys. The proposed TLACDAA is shown in Figure 1.

The first layer requires a user name, password and secret key. The second layer requires a Medium Access Control (MAC) address of a device. Device based authentication is used as a second level of authentication of data-owner. When the data-owner sign in, he is requested to connect his mobile device to scan its MAC address for the second level of authentication of the data-owner. If the attacker try to inject a spyware into the system, then the user's credentials can be learnt and system's authentication mechanism can be broken. To overcome the existing issue, a device based authentication is introduced in the second level authentication of proposed TLACDAA. The attacker need a hardware device of the data-owner which he fails to have.

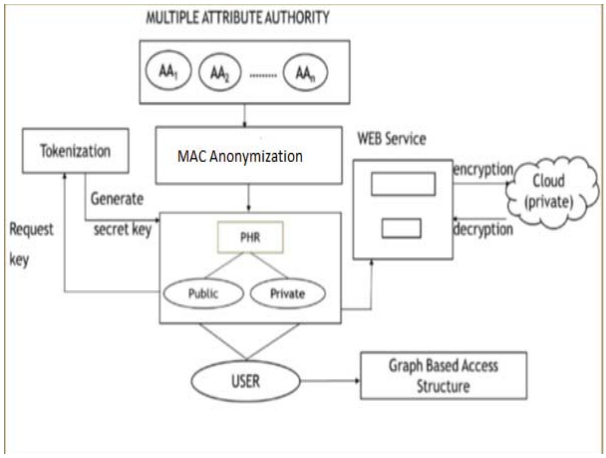

Fig. 1. Architecture of the Proposed TLACDAA

B. First Level Authentication

After the patient's registration, using tokenization technique, secret key is generated and sent to their registered mail id. The data-owner can sign in using their secret key for their first level of authentication, thereby uploading their data records or PHR file. The PHR file or data records are encrypted using master key that is generated during the upload of PHR file. The Personal health information are stored in the cloud in encrypted format for anonymous authentication. The user can download the PHR file and decrypt it only if they have access to master key. Access privileges are assigned based on the access control list. The cloud server has full access to the data-owner details and doctors. The cloud server can also add doctor and send them their credential details to their respective doctor mail id. The doctor can request for data access of patient details and data-owner can grant or revoke their request. If the request has been accepted then the master key of patient's PHR file is send to doctor mail id else the request is denied, thereby enforcing Denial Of Access (DOA) mechanism.

C. Proposed Improved Tokenization (I-TOK)

First level of authentication is performed as innovative and improved tokenization technique. Figure 2 explains about the first level authentication and the proposed tokenization technique named as Improved Tokenization (I-TOK) which is shown in Algorithm 1.

Algorithm 1: Improved Tokenization

Input: User ID (U_{id})
Output: T_k , HT_k

1. Register (Uid) ← RU_{id}
2. Pseudorandom number F((ε,ξ, φ) ⟶ T_k
   i) Function F = Rand(ε) + Rand(ξ) +Rand(φ)
   a) ε —— Randomized probability of occurring alpha character.
   b) ξ —— Randomized probability of occurring numerical character.
   c) φ —— Randomized probability of occurring special character.
3. Unique (Tk) ← Utdk
4. Send_Mail (Tk) ← SMk
5. Hash Token (Tk) ← HTk
6. Send_Mail (HTk) ← SMH(k)
7. First_Level_Authentication (Tk ,HTk)

TABLE I. NOTATIONS IN TOKEN GENERATION

Notation	Description
T_k	Token Key
HT_k	Hashed Token Key
U_{id}	User ID
SM_k	Sending Token to mail
Utd_k	Checking uniqueness of Token key

Once the users are registered, a token is generated. This token has randomized combination of special characters, numbers and letters along with timestamp. Token is generated in such a way, that it must be unique. The token is hashed by generating nonce as value pair for the token. The generated nonce is sent as secret key to the user's mail id. This secret key will be used for first level of secured authentication. The advantage of I-TOK is secret key is not shared directly in the database, thereby the cloud provider cannot find user's identity (anonymous authentication).

D. Second Level Of Authentication

Medium Access Control (MAC) anonymization is used as a second level of authentication of data-owner. When the data-owner sign in, he is requested to connect his mobile device to scan its MAC address for the second level of authentication of the data-owner. User's identity can be associated with the MAC address. The second level of authentication is shown in Figure 3 and device authentication is named as MAC Anonymization is explained in Algorithm 2.

Algorithm 2: MAC ANONYMIZATION

Input: MAC_Address→ MAC
Output: Hash_MAC_Address→H[MAC]

1. Per_Round_Shift
   s[]={7,12,17,22,5,9,14,20,4,11,16,23,6,10,15,21}
2. for i to 1 to 64
3. k[i] → floor(sin(i+1))
4. Buffer A=0x67452301
5. Buffer B=0xefcdab89
6. Buffer C=0x98badcfe
7. Buffer D=0x10325476
8. Append 1 to MAC(message)
9. for each 12_bit chunk of MAC(message)
10. Inter_buff A_1=A
11. Inter_buff B_1=B
12. Inter_buff C_1=C
13. Inter_buff D_1=D
14. Inter_buff F=0
15. for j1=1 to 64
16. buff_index=i
17. if 1 <=j1<=16
18. F=(B & C) | (~ B) & D)
19. else if 17<=j1<=32
20. F=(D & B) | ((~ D) & C)
21. g= (5*j1+1) mod 16
22. else if 33<=j1<=48
23. F = (B) ^ (C) ^ (D)
24. G = (3*j1 +5) mod 16
25. else if 49<=j1<=64
26. F = (C) ^ (B | (~ D))
27. G = (7*j1) mod 16
28. temp_buff=D

29. D=C
30. C=B
31. B=B + left rotate[(A +F + k[j1] + MAC[j1])], S[(j1 & 3) | j>>4)]
32. A=temp_buff
33. A+=A_1
34. B+=B_1
35. C+=C_1
36. D+=D_1
37. H[MAC]→ A Append B Append C Append D

TABLE II. OTATIONS IN MAC ANONYMIZATION

Notation	Description
Buffer A,B,C,D	Buffer Memory
Buffer A_1,B_1,C_1,D_1	Intermediate Buffer Memory
S	Round Shift Function
MAC	Mac Address
H[MAC]	Hashed MAC Address

MAC Anonymization is an idea of performing One-way hash function on a MAC address. The purpose of MAC Anonymization is to spoof the MAC address to prevent tracking of device owner's identity. The owner's movement can be easily tracked and his information can be leaked if the device owner's identity is found. In order to prevent user's identity being noticed, the MAC address is hashed and the hashed results are stored in the database. The hashing algorithm can be performed by taking 48-bit mac address as input and produces 128-bit output. The MAC Anonymization algorithm produces 128-bit word of hash value by dividing into 4 states of 32-bit word. The four 32 bit words are denoted by A, B, C, and D. The processing of 4 rounds are shown below

F(B,C,D) = (B & C) | (~ B) & D)

G(B,C,D)= (D & B) | ((~ D) & C)

H(B,C,D) = (B) ^ (C) ^ (D)

I(B,C,D) = (C) ^ (B | (~ D))

After these 4 rounds of operation, Left Rotation for 32 bit word A is performed using Round shift Function. All four 32 bit words A, B, C and D are appended to get the hashed result.

E. MULTI AUTHORITY CIPHER TEXT-POLICY ATTRIBUTE BASED ENCRYPTION (MACPABE) WITH ADVANCED ENCRYPTION STANDARD

In the proposed TLACDAA, after two layers of authentication, PHR files of data owner are to be outsourced in a cloud in an encrypted format. So MA-CPABE along with Advanced Encryption Standard (AES) is used for better privacy preservation. Multiple Attribute authority assigns access privileges to the user based on their role. Each Attribute authority encrypt certain set of attributes with the key and Attribute authority share the keys to those users who have access privileges to those attributes of the patient record. The Cipher text [17] is generated based on user's access policy. The access policy is defined by Graph based access structure.

Setup:

The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

Algorithm 3a: ATTRIBUTE BASED ENCRYPTION

Input: PT_{DATA} (A_i (i=1,2,3,...7)) , T_{KEY} , R_{ID}
Output: CT_{DATA}, A_{KEY} (i=1,2,3,...7) ,M_{KEY} (A_i (i=1,2,3.....7))

1) Master_Key_Generation (T_{KEY} , R_{ID}) ← M_{KEY}
2) for i=1 to 7
3) Attribute_key_Generation (A_i,M_{KEY}) ←A_{KEYi}
4) for i=1 to 7
5) if A_i is C_{high}
6) Encrypt_128_bit(PK,A_i,G) ⟶ $CT_{DATA}(A_i)$
7) else if A_i is C_{low}
8) Encrypt(PK,A_i,,G) ⟶ $CT_{DATA}(A_i)$

Algorithm 3b: ATTRIBUTE BASED DECRYPTION

Input: $CT_{DATA}(A_i(i=1,2,3....7))$, $A_{KEYi}(i=1,2,3....7)$, M_{KEY}
Output: $PT_{DATA}(A_i$ (i=1,2,3...7))

1) if (KEY==M_{KEY})
2) for i=1 to 7
3) if A_i is C_{high}
4) Decrypt_128_bit (A_i)⟶ $PT_{DATA}(A_i)$
5) else if A_i is C_{low}
6) Decrypt (A_i) ⟶ $PT_{DATA}(A_i)$
7) else if KEY = = A_i (i can be 1 to 7)
8) if A_i is C_{high}
9) Decrypt_128_bit(A_i) ⟶ PT_{DATA} (A_i)
10) else if A_i is C_{low}
11)Decrypt (A_i)⟶ $PT_{DATA}(A_i)$

F. GRAPH BASED ACCESS STRUCTURE WITH ABAC

In the existing system, tree based access structure is used. Graph Based Access Structure is designed for role attributes and data attributes. Here the role attributes refers to type of role of user. The role may be doctor, research analyst or patient. The data attribute refers to vital parameter details of the patient. Each node in the graph is the attribute (role or data) and they are connected by predicate. The predicate may be

AND, OR. Using attributes and predicates, access policies for the user are formulated.

TABLE III. NOTATIONS IN ATTRIBUTE BASED ENCRYPTION AND DECRYPTION

Notation	Description
PT_{DATA}	Plain Text Data Value
T_{KEY}	Token Key
R_{ID}	Record ID
M_{KEY}	Master Key
A_i	i^{th} Attribute value
A_{KEYi}	Attribute Key for i^{th} Attribute value
C_{high}	Attribute value in high criticality range
C_{low}	Attribute value in low criticality range
CT_{DATA}	Cipher Text Data Value

Graph Analysis:

Assumption: User U has access privileges for role attribute patient P and P1, hospital A, doctor (D_1 and D_2) and data attribute A_1 and A_2 of Patient P1, data attribute A_3 and A_4 of Patient P_2.

Access Privileges of User

$U=q_1+q_2+q_3+q_4$ (1)

Where q1, q2, q3 and q4 represent sub query. A graph access structure is shown in Figure 2.

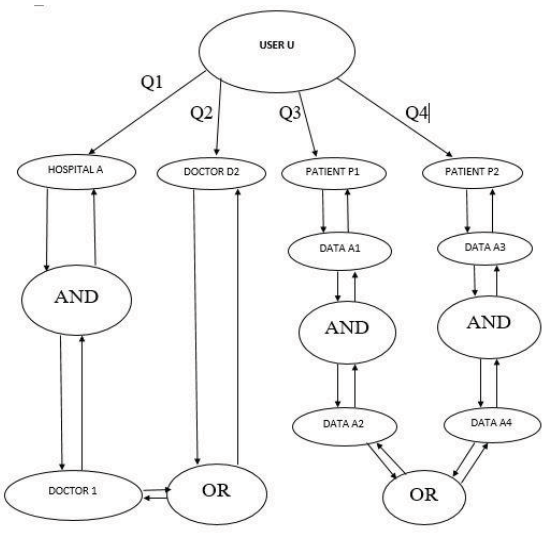

Fig. 2. Graph Based Access Structure

Consider User U as source node in graph G. Enqueue all the adjacent nodes of User U (source) and set it as visited in the queue initially.

Step 1:

Initial Queue

q_1	q_2	q_3	q_4
Hospital A	Doctor D_2	Patient P_1	Patient P_2

Step 2:

Enqueuing Adjacent nodes of q1 in a Queue

Hospital A	And	Doctor D_1	Or

Since no node in q1 has adjacent element, all the elements can be dequeued and appended to the result as q1

Therefore q1 = Hospital A and Doctor D1 or

Step 3:

Only 1 node is processed in q2 since all the nodes are already visited in q1

Therefore q2 = Doctor D2

Step 4:

Enqueuing adjacent nodes of q3 in Queue

Patient P_1	Data A_1	And	Data A_2	Or	Data A_4	And	Data A_3

Since no node in q3 has adjacent element, all the elements can be dequeued and Appended to the Result as q3

Therefore q3 = Patient P1 (Data A1 and data A2) or (Data A4 and Data A3)

Step 5:

Only 1 node is processed in q_4 since all the nodes are already visited in q_3

Therefore, q_4 = Patient P_2

From equation (1), Access Policy of User U = Hospital A and Doctor D_2 or + Doctor D_2 + Patient P_1 (Data A_1 and data A_2) or (Data A_4 and Data A_3) + Patient P_2

Access Policy of User U = Hospital A and Doctor D_1 or Doctor D_2 Patient P_1 (Data A_1 and data A_2) or (Data A_4 and Data A_3) Patient P_2

Thus Graph analysis is done using Queue data structure and policy is formulated for User U in a multi owner PHR environment. Therefore, considering the set of User U = {1, 2, 3… n}, the access policy can be formulated in the similar manner.

IV. RESULTS AND DISCUSSIONS

A. Implementation environment

The proposed TL-ACDAA based PHR is developed as a Web Application which includes health information of PHR users. The Zephyr dataset is taken for implementation. The Web application is deployed in Open Nebula [6] private cloud. Open Nebula is an open source management tool that helps virtualized data centres oversee private clouds. Open Nebula combines existing virtualization technologies. A virtual host is created with virtual network assigning the IP address for the instance of Virtual machine. Open Nebula includes various cloud performance parameter like CPU Cycles, Request per unit time etc.

B. Cloud Setup

The Web Application is deployed on the cloud server by creating VM instance in the Open Nebula private cloud. Two Layer Authentication is done on the cloud server. The user register their information and device on the proposed TL-ACDA PHR System and the secret keys are generated for the first and second level authentication. The user and device information for the corresponding registered user is stored in the MySQL database in cloud server. When the user request for access of the PHR setup, his credentials for first level of authentication is validated based on the information present on the MySQL database in cloud server. Then user's MAC address is scanned and the scanned result is validated with the MySQL database for the second level of authentication in cloud server. After getting access to the system, the user can upload their health records which is encrypted using MA-CPABE with AES in cloud server. The access policy of the users is formulated using Graph Based Access Control (GBAC). The records are encrypted using MA-CPABE with AES. Master Keys and Attribute Keys are generated for the uploaded PHR records and send to the registered Doctor's mail id. The doctors can access the patient's record by decrypting the patient's health data using master and attribute keys.

If any other user wishes to access the patient's record, they can request for the access of the records. The other users can access the records only if the patient (data owner) grant access to their request. Their request can also be revoked. If the access is granted, then the keys for the corresponding record will be sent to the requested user for accessing PHR information.

C. Security analysis

The proposed TLACDAA is sealed to collusion attack and replay attacks as discussed below.

a) Threat Model

The countermeasures to prevent or mitigate the effects of the replay attack and collusion attack for the proposed TLACDAA are as follows.

i. Collusion attack

Users individually illegitimate to access data combines their access policy to collude the scheme and decrypts data. This attack is predominant in system which has multiple attribute administrators working independently. The above discrepancy is overcome by having the global unique identifier in the proposed scheme. The secret keys of all users from different attribute administrators are fixed to his GID and thereby cipher text becomes autonomous from user's GID.

ii. Replay attack

Replay attack is a breakdown where the user who doesn't have a valid claim policy replaces fresh data with stale data. In the proposed TLACDAA, the session duration is encoded into the token of each user. The token obtained by the user is valid only for the encoded session duration, after which the user has to get authenticated again with the attribute administrators. Thus scheme is impermeable to both replay attack and collusion attack.

b) Attack Model

Theorem: The proposed TLACDAA scheme $\prod$ = (Global setup, Authority setup, KeyGen, Encryption, Decryption) [6] is secure under Bilinear Diffie-Hellman Assumption (BDH).

Proof:

Suppose there exist an adversary A' who can break our decentralized attribute based encryption scheme, there will exist an algorithm ƃ that can prove the Bilinear Diffie-Hellman assumption as follows:

Global setup:

The adversary A' will send a set of attributes $A_{data}(A_{d1}, A_{d2}, A_{d2}\ldots\ldots, A_{dn})$ which he wants to be challenged and A has some corrupted Attribute Authority C_A. A_{data} will be mapped a global Identifier GID

Authority setup:

There should be at least one attribute authority AA ¢ C_A where the adversary A' can get secret keys namely Master Keys (M_{KEY}) and Attribute Keys (A_{KEYS}) in the specified threshold range ƚ (k,n)

KeyGen:

Assume there exist 2 parties A and B along with the adversary A' under the attribute Authority AA ¢ C_A. The Attribute Authority AA generate secret keys. Let the secret keys be a_1, b_1 and a'_1.

Encryption:

Consider a message to be encrypted be M using a generator P, assume that challenger generate a bilinear map e between cyclic Groups G_1 and G_2 with P as generator of G_1.

TLACDAA scheme follows 3 functions:

- A → B,A$^{'}$:a_1M
- B → A,A$^{'}$:b_1M
- A$^{'}$→ A,B :$a_1^{'}$M

Based on Bilinearity in Groups G, $e(aM)^b = e(M)^{ab}$

Party A computes $e(b_1M, a_1^{'}M)^{a1} = e(M,M)^{a1b1a'1}$

Party B computes $e(a_1M, a_1^{'}M)^{b1} = e(M,M)^{a1b1a'1}$

Party A$^{'}$ computes $e(a_1M, b_1M)^{a1'} = e(M,M)^{a1b1a'1}$

All the parties have same key $K = e(M, M)^{a1b1a'1} \in G_2$.

Therefore, the protocol proved to be contingent for BDH assumption for encryption.

Decryption:

Similarly, the above protocol can be proved to be contingent for BDH assumption for Decryption.

Therefore, the proposed TLACDAA scheme ∏ = (Global setup, Authority setup, KeyGen, Encryption, Decryption) is secure under Bilinear Diffie-Hellman Assumption.

D. Performance analysis

a) Validation using AVISPA tool:

The Proposed TLACDAA is validated using Automated Validation of Internet Security Protocols and Applications (AVISPA). AVISPA is a tool for validating internet security protocol. The tool uses formal language CAS+. CAS+ is an expressive formal language for specifying security attributes and intruder knowledge. The tool is scalable to any standard security protocol and its performance is robust. To validate the replay and collusion attack, the role of the user, list of keys and the number of intruders in the system are specified as a pre-requirement to the tool. Association rules are composed as knowledge to the system. Apart from association rules, the intruder knowledge of the system is also given and the number of nonces sent on the session are specified on the session instance. The protocol is validated using in-built tool HLPSL (High Level Protocol Specification Language). The validated results are shown in Figure 3.

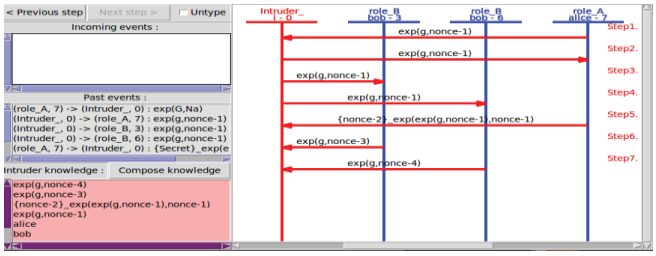

Fig. 3. AVISPA validation

V. CONCLUSION

A Cloud based two layered access control with decentralised anonymous authentication is proposed which prevents replay attacks and MA-CPABE based AES is implemented in the proposed TLACDAA to ensure privacy preservation. Graph Based Access Structure is used by incorporating hidden access policy for fine grained access control. Open Nebula Cloud is deployed which ensures remote access of proposed TLACDAA system. For ensuring better privacy preservation, data owner is anonymously authenticated using enhanced tokenization. The Confidentiality of the system is improved using MAC Anonymization. Moreover, the proposed TLACDAA is validated using AVISPA tool. From the validation results, it is found that the proposed scheme is resistant against security attacks.

VI. FUTURE WORK

The backend database used for the system is MySQL which is an open source relational database management system designed to manage data across multiple commodity resources. However, the proposed TLACDAA can be implemented using other NoSQL database for higher scalability and superior performance. The advantage of using NoSQL database is able to include large volume of structured, semi-structured and unstructured data. The proposed TLACDAA ensures only confidentiality by providing fine grained privacy preservation however the system does not perform any integrity check. Therefore, using any digital signature technique integrity check can be performed in the system.

REFERENCES

[1] Agrawal, R., Kiernan, J., Srikant, R., Xu, Y.: Order-preserving encryption for numeric data. In: SIGMOD 2004, pp. 563–574. ACM, New York (2004)

[2] Amit Sahai, Vipul Goyal, Omkant Pandey, Brent Waters “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data” IEEE Transactions On Parallel And Distributed Systems Year 2005.

[3] B. Wang, W. Song, W. Lou and Y. T. Hou, "Inverted index based multi-keyword public-key searchable encryption with strong privacy guarantee," 2015 IEEE Conference on Computer Communications (INFOCOM), Kowloon, 2015, pp. 2092-2100.

[4] Boldyreva A,Chenette N,Lee Y,O’Neill A. (2009) “Order-Preserving Symmetric Encryption”,Advances in Cryptology - EUROCRYPT 2009. Lecture Notes in Computer Science, vol 5479.

[5] CHEN Danwei, CHEN Linling, FAN Xiaowei, HE Liwen, PAN Su, Hu Ruoxiang,” Securing Patient-Centric Personal Health Records Sharing System in Cloud Computing”,IEEE,2013.

[6] Han, Jinguang, Willy Susilo, Yi Mu, and Jun Yan. "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption", IEEE Transactions on Parallel and Distributed Systems, 2012

[7] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, “A secure cloud computing based framework for big data information management of smart grid,” IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.

[8] Joseph K. Liu, Man Ho Au, Xinyi Huang, Rongxing Lu, “Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services, IEEE Transactions on Parallel and Distributed Systems, MARCH 2016

[9] Kandasamy.V, 2 Papitha.E," Flexible Access Control for Outsourcing Personal Health Services in Cloud Computing using Hierarchical Attribute Set Based Encryption", IEEE,2013.

[10] K. Liang et al., "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.

[11] Kaitai Liang, Liming Fangy, Willy Susiloz, and Duncan S. Wong," A Ciphertext-Policy Attribute-Based Proxy Re-Encryption with Chosen-Ciphertext Security".

[12] Ming Li Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption",2012.

[13] N. Cao, C. Wang, M. Li, K. Ren and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222-233, Jan. 2014.

[14] Qinqin Wang, Yanqin Zhu*, Xizhao Luo,"Multi-user Searchable Encryption with Fine-Grained Access Control without Key Sharing", 2014 3rd International Conference on Advanced Computer Science Applications and Technologies.

[15] Soubhagya B, Venifa Mini G, Jeya A. Celin J "A Homomorphic Encryption Technique for Scalable and Secure Sharing of Personal Health Record in Cloud Computing" International Journal of Computer Applications (0975 – 8887) Volume 67– No.11, April 2013.

[16] Z. Xia, X. Wang, X. Sun and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," in IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340-352, Feb. 1 2016.

[17] ZHANG Ya-ling, Liu Kai, WANG Shang-ping, Sun Qin-dong,"A Multi-users Searchable Encryption Scheme with Proxy Re-encryption", 2014 10th International Conference on Computational Intelligence and Security.

[18] Zhongma Zhu and Rui Jiang," A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud",IEEE Transaction,January 2016.