of them will include additional functionality to accomplish the objective of this proposal. In the following, an enumeration of these elements and a brief description of their functionality are presented. Figure 1 shows the elements of the architecture and the protocols that allow communication between each pair of entities.

3.1.1 End User
This entity represents an end user that first authenticates to access the network service provided by visited institution using eduroam/DAMe and, after that, desires to access services.

3.1.2 Radius Server in the home institute
This component is already present in the eduroam architecture. It communicates with the IdP.

3.1.3 Radius Server in visited institute
This component is also already present in the eduroam architecture. It communicates with the IdP. And user request is transported through this server to the respective institute.

3.1.4 IDP
This component, defined in the DAMe architecture, is responsible for providing both end user's attributes to the requesting parties and eduToken to the home RADIUS server after a successful authentication of the end user.

3.1.5 eduToken
This is a type of packet which consist of detail information about end user.

3.1.6 Access Point
This component is present on eduroam and acts as the point of attachment to the visited institution's network. It interacts with the RADIUS infrastructure to authenticate the end user and provides network connectivity after a successful authentication.

3.1.7 TGS
TGS (Ticket granting Server) is responsible for granting ticket to the end user so that the user can access different types of services in the visited institution.

3.1.8 PDP
It manages the access control policy set of the visited institution.

3.2 System Architecture

Eduroam that is education roaming is a network of network federations which is generally developed for researchers, students and staff from institutions which are part of eduroam network i.e. participating institutions. The eduroam framework supports user authentication and essential authorization systems, the DAMe (Deploying Authorization Mechanisms for federated administrations in eduroam building design) is basically used for the proposition of enhancing the federated network access situation of eduroam. Kerberos is nothing but, a protected three party protocol for authentication also key administration focused on shared secret key cryptography. Kerberos is a standard protocol which is turning into amongst the most generally deployed for authentication and key distribution in application administrations. The fundamental objective of our work is to process an authentication and authorization framework for federated administrations facilitated in the eduroam network. The basic aim of DAMe is to give progressed authorization administrations to eduroam considering not just the end user authentication process, additionally extra features like privilege, roles etc. which are assessed before giving or denying network access.

In our work, the member of institution can access the internet from any institution which is part of the eduroam by using his own credential of home institution and also able to access other services which may be provided by visited institution. Indeed it is very important to define some access control mechanism to access these services provided by visited institution. In this article this paper proposes advanced authorization based on user attributes that are defined in his home institution that are used to provide services to the end user who is roaming from his home institution. This work additionally proposes the dissemination of an authentication token, which is proposed to be utilized for access to other services, along with the cross-layer SSO (Single Sign-On). In our work, we have provide different authorities to various types of users in our system. So that priorities can be set to every user. We are focusing on attribute based authorization. So, according to parameterized access control user priority is set.

In this architecture the end user enters username & password in the browser then both the details proceeds to TGS server. The IDP block receives the user details and access the relevant data form idP. The encryption [17] process starts after accessing the data and revert back to the TGS server in encrypted form. In this operation one secrete key is generated for privacy purpose. After that the data move on to Radius server and contents referred with PDP. Now the existing data decrypted. The user provided password compared with available data content. If both the data matched then user can get access to Radius server.

Depending upon the user role in his home institute user get services. As a example for web service we have taken internet as example and for non-web service we have taken database as a service. On can take printer as a hardware as a service. Figure 1 shows the proposed system architecture.

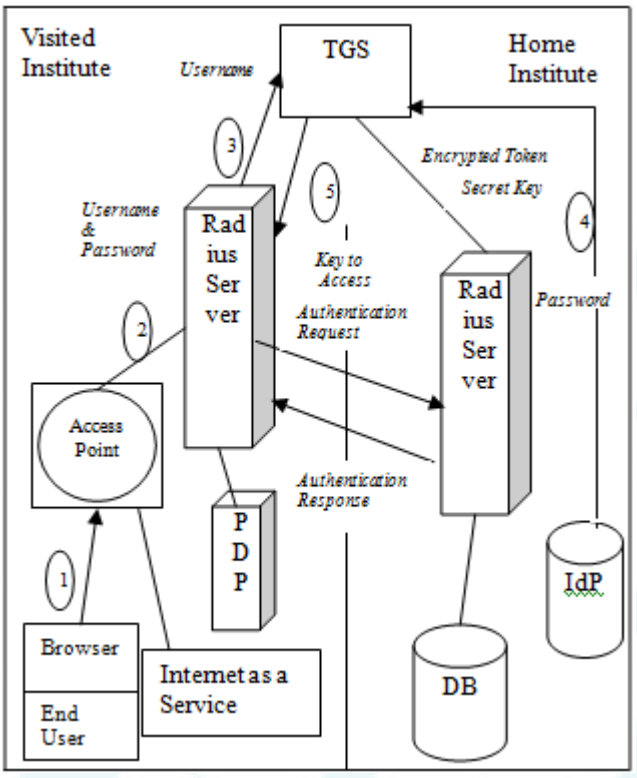

Figure 1: Proposed System Architecture

3.3 Algorithm

Following are the algorithms [7] used in our propoed system.

The following notations are used below in the algorithms.
Where,
AP- Access Point
EU- End User
IDP- Identity Provider
EAP- extensible authentication protocol
VR- Visited Institution Radius Server
HR-Home Institution Radius Server
PDP- Policy Decision Point
KDC- Key Distribution Center.
TGS – Ticket Granting Servers.

For network authentication following process is done.

1. System →: AP: Start
2. AP→EU:eap_req
3. EU→AP:eap_res
4. AP→VR:[Access-Request(anonymous@home,eap-res)]
5. VR→HR:[[Access_Request(anonymous@home,eap-res,keying material, randomizer,mac)]Mackey_vr_hr]
6. HR→VR:[Access_Challenge (anonymous@home, eap-req)]
7. VR→AP:[Access_Challenge (anonymous@home, eap-req)]
8. AP→EU: eap_req
9. Repetition of steps from 1 to 7. After several steps HR finalize the authentication.
10. VR→HR:[[Access_Request(anonymous@home,eap-res, keying material, randomizer,mac)] Mackey_vr_hr]
11. HR→IDP: {AuthnRequest(username)}HR-1} IDP
12. IDP→HR:{{SAML Response(eduToken)}IDp-1} HR
13. HR→EU:{edu token}tk
14. HR→VR:[[Access-accept(emsk_name, eap_succ,psuedonym,msk, {keying_material(dsrk)randomizer mac}mackey_vr_hr)
15. VR→AP:[Access-Accept (emsk_name, eap_succ, pseudonym, msk)]
16. AP→EU:eap_succ

Steps for Kerberos pre-authentication and TGT acquisition are as follows.

1. System →End User: Start
2. EU→KDC:AS_REQ(WELL-KNOW:ANONYMOUS, PA_PK_AS_REP (dh_eu))
3. KDC→EU:AS_REP(WELL-KNOW:ANONYMOUS, PA_PK_AS_REP(dh_kdc,{sign_data}KDC-1}
4.EU→KDC:AS_REQ(WELLKNOWN_FEDERATED,PA_FX_FAST_REQUEST({armor_TGT}key_as_tgs{enc_fast_req(PA_EDUTOKEN(eduTOKEN, emsk_name, [ts]reply_key), req_body)}armor_key))
5. KDC→VR:Access_Request(emsk_name, keying_material,randomizer,mac)]Mackey_kdc_vr]
6. VR→KDC:[[Access-Accept(emsk_name, {keying_material(dsusrk)}keymat_key_kdc_vr, randomizer, mac)]Mackey_kdc_vr]
7.KDC→EU:AS_REP(pseudonym,PA_FX_FAST_RESPONSE({enc_fast_rep}armor_key),{TGT(eduToken,session_key)}key_as_tgs, {enc-part(session-key)}reply_key)

Following are the authorization and ST acquisition steps.

1.EU→KDC:TGS_REQ(service,TGT(eduToken,session_key)}key_as_tgs,{authenticator}session_key)
2.KDC→IDP:{{AttributeQuery(pseudonym, service)}KDC-1)IDP}
3. IDP→KDC:{{SAMLResponse(attributes)}IDP-1}KDC
4. KDC→PDP: {{Authorization Decision Query(service, attributes)} KDC-1}PDP
5. PDP→ User: {User_type, authority attribute}User type – Student, Principal, Admin. Authority attribute-Modify,change, View, Read, Write, All access.
6. PDP→KDC: {{Authorization Decision Response(decision, obligation)PDP-1}KDC
7. KDC→EU: TGS_REP (pseudonym, {ST(service_session_key)}service_key,{enc-part (service_session_key)}session_key)

4. Proposed Algorithm

Following is the algorithm used in our proposed system.
1: End User ⟶ AP: Start
2: AP ⟶ EU: request for username and password
3: EU ⟶ AP: username and password
4: AP ⟶ VR :[Access-Request(TGS)]
5: VR ⟶ HR and TGS: [Access Request(username]
6: Symmetric Key Encryption
- HR and TGS ⟶VR:[Encryption(Key, Password)]
- TGS Encryption Process Using AES Algorithm

7: Decryption process
if(Decryption successful)
{
Authentication Successful
}
else

{
Authentication FAIL
}
8: Repetition of steps from 1 to 7. After several steps HR finalize the authentication.
9: HR ⟶ PDP: [Authorization]
9: IDP ⟶ HR: [Depending upon the privileges of End User]
10: VR ⟶ AP: [Access-Accept]
11: AP ⟶ EU: Successful

5. Mathematical Model

The system S is represented as:
S = {A, T, C, P}

a. Authentication

Consider A = {S, R}
i. client sends request to AS
Let S is a set of request sends
S = {s1,s2,s3…}
Where,
s1,s2,s3.. are the no of requests.
ii. AS respond for request to client
R = {r1,r2,r3…}
r1,r2,r3…. are the number of responds.

b. Token Generation

Let, T is a set of token generation for session
T = {t1,t2,t3,….tn}
Where, t1,t2,t3…are the number of tokens.
iii. Client request for token and token sends to client

c. Client Communication with Application Server

Let C is a set of communication happen between client and AS
C = {c1,c1,…..}
Where, c1,c2.. are the number of communication done between them.

d. Advanced Authorization

consider, P is a set for priority wise advanced authorization.
P = {p1,p2,…..}
Where, p1,p2,…are the number of priorities assigned

6. Experimental Results

In this section the results are taken by setting the eduroam architecture using two system. One system is playing as home institute role and other as visited institute role. The two systems are connected using Ethernet Lan cable. Following is the graph plotted as on x- axis we have taken different entities related to roaming end user and on y-axis time. Below graph shows details.

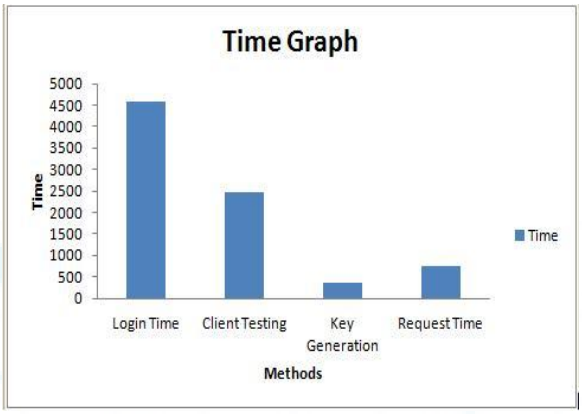

Figure 2: Resultant Graph

7. Conclusion

This paper describes how the worldwide spread eduroam system can be reached out to provide end user access to federated advantages past the web. DAMe offering gives consent what's more token circulation to establishments ready to offer added worth system access management to meandering clients. Also we describes how the roaming user attributes are used for accessing federated added value service in the visited institution and depending upon the role of user in home institution. By integrating the eduroam architecture in the Kerberos protocol. This kerberos protocol helps to achieve the eduroam properties or characteristics. As a example for web service we have taken internet as service example and for non web service we have taken database as service. As a future work one can think of integrating eduroam architecture using public key cryptography in kerberos protocol. And also more advanced authorizations can be achieved using roaming user attributes.

References

[1] Arias-Cabarcos, Patricia, Almenarez-DAMe Project. http://dame.inf.um.es.
[2] GEANT Project. http://www.geant.net/pages/home.aspx.
[3] Neuman, C., Ts'o, T.: Kerberos: An Authentication Service for Computer Networks. IEEE Communications 32 (1994) 33–38
[4] Neuman, C., Yu, T., Hartman, S., Raeburn, K.: The Kerberos Network Authentication Service (V5) (2005) http://www.ietf.org/rfc/rfc4120.
[5] Thomas, M., Vilhuber, J.: Kerberized Internet Negotiation of Keys (KINK) (2003) http://ietfreport.isoc.org/all-ids/draft-ietf-kink-kink-06.txt.
[6] Kohl, J., Neuman, C.: The Kerberos Network Authentication Service (V5) (1993) http://www.ietf.org/rfc/rfc1510.
[7] Alejandro Pérez-Méndez, Fernando Pereñíguez-García, Rafael Marín-López, Gabriel López-Millán, "A cross-layer SSO solution for federating access to kerberized services in the eduroam/DAMe network" International Journal of Information Security, Springer-Verlag November 2012, Volume 11, Issue 6, pp 365-388 Date: 23 Aug 2012.

[8] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.: Extensible Authentication Protocol (EAP). RFC3748, June 2004.
[9] Marín-López, Rafael, Pereníguez, Fernando, López, Gabriel, Pérez-Méndez, Alejandro: Providing EAP-based Kerberos preauthentication and advanced authorization for network federations. Comput. Stand. Int. 33(5), 494–504 (2011)
[10] Hartman, S., Howlett, J.: A GSS-API Mechanism for the Extensible Authentication Protocol. IETF Internet Draft, IETF draft-ietfabfab-gss-eap-04.txt, October 2011.
[11] Howlett, J.:A RADIUS Attribute, Binding and Profiles for SAML. IETF Internet Draft, IETF draft-ietf-abfab-aaa-saml-02.txt, October 2011.
[12] Wei, Y.: Federated Cross-Layer Access. IETF Internet Draft, October 2011.
[13] Zhu, L., Jaganathan, K., Hartman, S.: The Kerberos Version 5 Generic Security Service Application Program Interface (GSSAPI) Mechanism: Version 2. IETF RFC 4121, July 2005.
[14] Melnikov, A.: The Kerberos V5 ("GSSAPI") Simple Authentication and Security Layer (SASL) Mechanism. IETF RFC 4752, November 2006.
[15] Wen-Guey Tzeng Jianying Zhou Cheng-Kang Chu, Sherman S. M. Chow and Robert H. Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. Parallel and Distributed Systems, IEEE Transactions, Volume(106):468- 477, 2014.
[16] Howlett, J.: Hartman. Project Moonshot, S. (February 2010).
[17] William Stallings. Cryptography and Network Security Principles and Practice. (FifthEdition).
[18] G. Lopez, O. Canovas, A. F. Gomez-Skarmeta, and M. Sanchez, "A proposal for extending the eduroam infrastructure with authorization mechanisms," Computer Standards Interfaces, Elsevier BV, vol. 30, pp. 418–423, 2008