International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

A Novel Collaborative PKI Framework in Public Cloud

Ashok Kumar J, Gopinath Ganapathy

Abstract: ***Public Key Infrastructure (PKI) is a repository and management system for digital certificates. It can be the centralized or decentralized PKI system for issuing, managing, storing, verifying and distributing the key pairs, public key and private key, or one of the public key certificates. In public cloud, Data Owners and Data Users can upload or download their encrypted data along with services, resources and infrastructures in the hands of Cloud Service Provider. It creates the big security concerns in terms of data security and data privacy for the user and Cloud Service Provider is the sole responsibility to provide the Access Control Policy to restrict the cloud services centrally. With the emergence of cloud computing, Public Key Infrastructure (PKI) technology enables the secure communications in between systems. X.509 certificates are based on the centralized PKI and suffers so many issues in the public cloud. Gnu Privacy Guard (GnuPG) certificates are based on the decentralized PKI system. Imagine a world with decentralized PKI system in which each Kerberos is also a Central Authority for issuing certificates to the system or users. This proposed collaborative PKI framework describes the use of PKI in public cloud, proposed algorithm for Kerberos SSO token and provides acquisition of Public Key certificates from the client via Kerberized Central Authorities.***

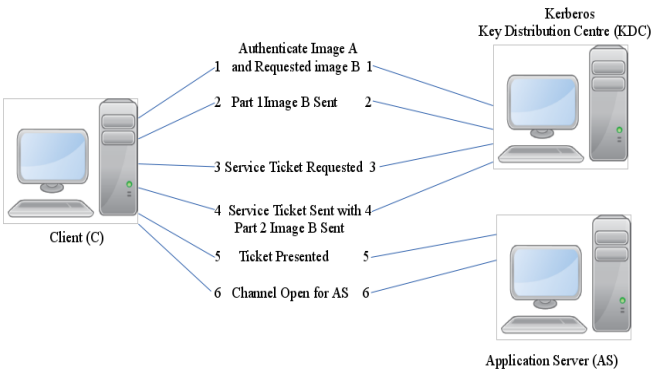
Keywords: Public Cloud, Kerberos Authentication, Kerberos SSO token, X.509, GnuPG , PKI.

I. INTRODUCTION

The Cloud computing is a distributed computing paradigm, it provides the application services and resources to the users on pay-per use basis. The users outsource their data for computation in public cloud server and it results they are losing the physical control over the data. They are unable to resist certain type of attacks and threats over them. To secure the users data in public cloud, the Cloud Service Providers (CSP) shall protect the cloud server from different type of threats and attacks. It should be ensured that the CSP is trusted with the user before outsourcing the user's data. The modified Collaborative Trust Enhanced Security (CTES) model [1] has an inbuilt access control mechanism for Kerberos protocol itself to enforce the access control policy directly into the Client system node and altered the Kerberos Authentication based on secret image and GnuPG Certificate. Data confidentiality for the stored data in public cloud is achieved by cryptographic techniques. Gnu Privacy Guard (GnuPG) based certificate is capable enough to verify the identity of the correspondent in information exchange as well as the information integrity. It is a strongest authentication technique where the user is asked to provide his/her digital ID for validation in the Server and enables Single sign-on services for Kerberos Authorization in modified CTES model. In this paper, it is proposed a novel Collaborative PKI (CPKI) framework based on GnuPG certificate in Public Cloud.

II. MODIFIED KERBEROS V AUTHENTICATION

In paper [2], the Kerberos protocol incorporates with Visual cryptography and GnuPG Public key Cryptography for client-based authentication (Fig I). The Visual cryptography is used for enforcing the access control mechanism to authenticate the user through secret image. To securely exchange the secret image between the client and KDC, the



(Fig I: A Modified Kerberos V Authentication)

GnuPG public key is used to encrypt and decrypt it. Moreover, the client private key is available in the client system itself and so the only responsibility of client to decrypt the image. It is more secure than the traditional authentication and secret image can hold enough data for access control information about the authenticating user to enforce it into the client system directly.

Each client generates the GnuPG private key and public key by itself in the secure manner and it is stored securely with the paraphrase in the client system itself. Then the public key alone and not the private key can be shared with the super host for secure communication in the Public Cloud. The proposed CPKI framework is based on the Modified Kerberos V Authentication model.

Manuscript published on January 30, 2020.
* Correspondence Author
Ashok Kumar J*, Research Scholar, Bharathidasan University, Engineering and Applications, School of Computer Science, Tiruchirappalli, India.
Dr. Gopinath Ganapathy, Registrar, Bharathidasan University, Tiruchirappalli, India.

III. FEATURES OF MODIFIED KERBEROS V AUTHENTICATION

A Novel CPKI framework belongs to the below Modified Kerberos V Authentication features [2]:

1. The Visual Cryptography is used as a pre-authentication for AS and TGS and so the user authentication is based on one part of the secret image "shared image A". But the other part of the "shared image A" is kept in TGS server itself and never disclosed with any system or any user.
2. The authorization access policy for client is based on second Secret image "shared image B". After the successful authentication, the access control mechanism is enforced for the authenticated user.
3. Each client generates the GnuPG private key and public key by itself in the secure manner and it is stored securely in the client system itself. Private key is protected with passphrase.
4. To prevent the replay attack, sequence number mechanism is utilized instead of timestamp mechanism.
5. Password guessing attack is not possible because one-time password (OTP) is used, instead of the client password.
6. Each process in the system is verified with the Digital Signature mechanism by using public key encryption. If any of the user is impersonated, then it will not compromise for all the user in this infrastructure.
7. When the Kerberos server is down, the GnuPG certificate authenticates the user with the private key in the system itself and results to get log in to the system. Kerberos server does not require continuous availability for authorizing the users.
8. This approach resolves the problem in distributed systems for computation of data in the node by enforcing access control mechanism within Kerberos protocol itself for ensuring data security and privacy of the data in that system.

IV. PUBLIC KEY INFRASTRUCTURES (PKI)

It is the concept of key distribution and management. Certification Authority (CA) is hierarchy based X.509 PKI for securely associating a key with user (or email address), PGP/GnuPG proposes the concept of Web of Trust, the users can generate the certification in the client system itself so that it avoids for a single certification authority [3].

A. Digital signatures

A digital signature mechanism in the public key helps to identify the sender and provides the features of non-repudiation. The receiver is able to verify if information is intact. It also provides data integrity and authentication for this proposed CPKI model [3].

B. Digital certificates

Digital certificates incorporate public key and other user information for establishing the relation in between the user and public key. It is used to encrypt the data for the recipient [3].

C. Fingerprint:

A long public key is identified using a short sequence of bytes named as fingerprint. These short sequences of bytes are calculated with the use of cryptographic hash based on the public key. In this proposed CPKI framework, fingerprint is used to validate the public certificates [3].

D. Key Server

A key server is a database that allows users to submit and retrieve their public key. It provides the storage management and key management features like store, retrieve and trust for public key called Public Key Infrastructures (PKI). These public key certificates are utilized by the user for exchanging their data securely [3].

E. X.509 CERTIFICATE

It is based on the Certification Authority (CA) defines a framework for the provision of authentication services to its users. Each certificate contains the public key of the user and it is signed with the private key of a trusted CA[3].

X.509 certificates have the following data:

- The X.509 version number
- The certificate holder's public key
- The serial number of the certificate
- The certificate holder's unique identifier
- The certificate's validity period
- The unique name of the certificate issuer
- The digital signature of the issuer
- The signature algorithm identifier

The user has to request CA to issue a certificate by providing the signed public key. Then CA verifies the provided information and generate the certificate.

F. GNU Privacy Guard (GnuPG)

PGP was developed by Philip R. Zimmermann [4]. GnuPG is an open source compatible encryption system based on OpenPGP. PGP/GnuPG encryption, uses combination of public key cryptography, data compression, hashing and symmetric-key cryptography. It is used in several security constraints such as confidentiality, integrity and authentication for electronic mail and file storage applications etc., [5]. GnuPG creates the digital signature for the given data to verify the authenticity of the sender. Sender sends the hash digest along with the given data to the receiver. Then receiver uses the sender's public key to verify the digital signature. If it matches the digital signature, it will be confirmed that it is from the expected sender. GnuPG subkeys [6] are like the normal key pair associated with the main key pair used for signing or for encryption except they're bound to a master key pair. It can be revoked independently of the master keys, and also stored separately from them.

A PGP certificate contains the below data:

- The PGP version number
- The certificate holder's public key
- The certificate holder's information - consists of "identity" information about the user

- The digital signature of the certificate owner - this signature using the corresponding private key of the public key associated with the certificate.
- The certificate's validity period - start date/time and expiration date/time of the certificate.

Web of Trust is a decentralized public key infrastructure in which each user can "introduce" public keys with different levels of trust indicating how trustworthy the signature of the certificate holder. The four trust levels are existing in users certificate holder's signature to introduce other users' certificates:

- Mode Level 4: Fully trusted
- Mode Level 3: Marginally trusted, but to confirm with full trust
- Mode Level 2: Untrustworthy
- Mode Level 1: Don't Know

V. SHAMIR'S SECRET SHARING SCHEME

In Shamir's Secret Sharing scheme [11], Shamir is proposed that k points are divided in to m shares such that other party requires the same m shares to get the information. If other party receives less than the m shares that is m-1 shares, they cannot retrieve the original information. This is called the threshold, and is used to denote the minimum number of shares needed to unlock the secret. This scheme is advantageous because there is no decryption algorithm is needed and even infinite computing power will not predict the message. In this proposed methodology, Kerberos SSO token T can be divided into k points of data $T_1, T_2,...,T_k$ such that m shares are enough for decryption based on the below mathematical definition :

1. If m<k, then m shares are needed for decrypting the SSO token T. For example, if m=3, k=5, then 3 shares are enough to decrypt the SSO token T.
2. If m=k, then all the shares are needed for decrypting the SSO token T.

A. Threshold Cryptography Algorithm:

Let us take (m, k) threshold scheme to distribute the Kerberos SSO token T. Among them, choose random m-1 coefficients and let they are as $T_0, T_1, T_2, T_3,....., T_{m-1}$. Assume that T_0=T. Now divide the Kerberos SSO token T by picking a random degree polynomial as follows,

$Q(x) = T_0 + T_1 x + T_2 x^2 + T_3 x^3 + ... + T_{m-1} x^{m-1}$

The subsets of m number of pairs can find secret s , by using interpolation Method. The secret is the constant term of that interpolation equation which is T_0.

To evaluate the above expression,

Let's S=2469, n=7, m=3

Randomly selected two numbers: T_1=207, T_2 = 86 which are used to make the polynomial:

$Q(x) = 2469 + 207 x + 86 x^2$ → equation no(1)

Now, from equation (1) we can get 7 separate points for x=1, 2, 3 ……7.

When x=1 then Q(1)=2762
When x=2 then Q(2)=3227
When x=3 then Q(3)=3864
When x=4 then Q(4)=4673
When x=5 then Q(5)=5654
When x=6 then Q(6)=6807
When x=7 then Q(7)=8132

So, seven points are obtained from the polynomial: (1, 2762); (2, 3227); (3, 3864); (4, 4673); (5, 5654); (6, 6807); (7, 8132). So that each participant can get different single point (both x and Q(x)).

B. To reform the secret:

In order to reform the secret S, m points will be enough. Let m=3 and consider (3, 3864); (5, 5654); (7, 8132). It is possible to form Q (x) again by using Lagrange's polynomial, and the value of T can also be retrieved which is same as before.

Let us consider (x0, y0) = (3, 3864); (x1, y1) = (5, 5654); (x2, y2) = (7, 8132). Lagrange's polynomials can be computed as:

$$L_0 = \frac{x-x_1}{x_0-x_1}.\frac{x-x_2}{x_0-x_2} = \frac{x-5}{3-5} \cdot \frac{x-7}{3-7} = \frac{1}{8}.x^2 - 1\frac{1}{2}.x + 4\frac{3}{8}$$

$$L_1 = \frac{x-x_0}{x_1-x_0}.\frac{x-x_2}{x_1-x_2} = \frac{x-3}{5-3} \cdot \frac{x-7}{5-7} = -\frac{1}{4}.x^2 - 2\frac{1}{2}.x + 5\frac{1}{4}$$

$$L_2 = \frac{x-x_0}{x_2-x_0}.\frac{x-x_1}{x_2-x_1} = \frac{x-3}{7-3} \cdot \frac{x-5}{7-5} = \frac{1}{8}.x^2 - x + 1\frac{7}{8}$$

$$F(x) = \sum_0^2(x)\, y_i l_i \quad \text{.....(2)}$$

Now by using the above equation (2), we can reform our secret in this way,

$$F(x) = 3864(\tfrac{1}{8}.x^2 - 1\tfrac{1}{2}.x + 4\tfrac{3}{8}) + 5654(-\tfrac{1}{4}.x^2 - 2\tfrac{1}{2}.x + 5\tfrac{1}{4}) + 8132(\tfrac{1}{8}.x^2 - x + 1\tfrac{7}{8})$$

$$= Q(x) = 2469 + 207x + 86x^2$$

After necessary calculations we get the same equation as equation no (1) Remember that the secret is the free coefficient, which means that S= 2469, and as it is similar to the equation (1).

VI. RELATED WORKS

Natasa prohic had proposed the differences in certificate for PGP certificates and PKI certificates [7]. PGP public certificate has multiple signatures values whereas PKI certificates has a single signature. PKI certificate allows single name for each owner but PGP uses the different labels to identify several users.

Based on X.509 concept [8], CA issues the certificate to the end user and the certificate validation is based on "Chain of Trust". Root CA certificate is a parent CA for the leaf CA in hierarchy level to validate all the certificates.

A secure communication is proposed by Xiaowei et al. [9] between user and CSP. The main problem of this scheme is that the Data Owner (DO) should always be online when user wants to access data. PGP is initially created as an e-mail encryption tool and it protects two corresponding parties in a secure channel with the use of public key. Users are allowed to trust a public-key certificate in two ways, firstly in its validity as a correct binding between the public-key and the claimed owner of that key, and secondly as representing the key of a trusted introducer [10].

VII. X.509 PROBLEM STATEMENTS

The following limitations are in the X.509 certificates.

1. If the keys are compromised, then the distribution of the revoked key takes longer time and it results in no guarantee that a particular key belongs to an identified user at a particular moment in time.
2. Certificate Authority checks the certificate through online. So, it is possible to know the entire history of user interactions and it is violation of user's privacy.
3. It is possible to create certificate in an identical name at different Root CA.
4. To update the user certificate, it requires repeated access to the registration center for reissuing the certificate, changing the data, and then verifying often with the Certificate Authority.
5. The possibility of single point of failure for centralized server will result in compromising of Root Certificates.
6. Central Authority has full authorities over identifiers and not in the hands of actual owners.
7. In case of scattered companies, the centralized X.509 PKI does not scale to support a large community of partners. Therefore, in case of health organizations where multiple hospitals may need to exchange data like e-mails with multiple patients and with multiple hospitals, it's not advisable to adopt this centralized PKI for securing the individual user's data.

VIII. GNUPG ADVANTAGES

The following advantages are in the PGP certificates.

1. If the private key is not compromised, then it is ensured that the intended participant can only read the message.
2. With the help of web of trust model, the user can decide the trust relationship with other users instead of from the central authority.
3. The sub public key is associated with the master public key which assists for the backup of master key to resolve the issues like losing or unknowingly deleting the user private key.
4. The fingerprint is used to verify the user's public key.
5. It uses digital signature as the introducer for trusting the user within the domain. Since the user can directly communicate with other domain users, it does not need the cross certification in between the different domains.

IX. IDEA BEHIND THIS PROPOSED COLLABORATIVE PKI (CPKI)

PKI is a framework to provide public key certificates. OpenPGP supports both public-key cryptography and symmetric key cryptography. PKI is based on certificate authorities (CA) whereas OpenPGP depends on a web of trust model [20]. The users in the OpenPGP can choose whom they trust, whereas users in a PKI system has to depend on trusted CA. The main limitations of X.509 certificate is explained in the section "X.509 Problem Statements" and will not be considered for the proposed CPKI framework. Kerberos protocol is utilized as a central Authentication and Authorization server to the web of trust model. Integration of centralized trust mechanism of Kerberos with decentralized model of PGP yields the novel CPKI framework to mitigate the issues identified in this paper.

X. IDEA BEHIND THE GENERATION OF KERBEROS SSO TOKEN:

Consider the Kerberos Server generates SSO tokens T_1 , T_2 , T_3, T_4, T_5 , T_6 and T_7 from the secret T(also called T_0). These tokens are getting stored at KDC itself. Cloud Service provider can decide the authorization policy to provide access control information to client and resource server. If m is taken as 3, then the SSO tokens such as T_1 and T_2 will be transferred into resource server. Client will receive any one of the tokens such as from T_3 To T_7. Finally, the client will submit the SSO token $T_{3\text{-}7}$ into resource server to gain access the resources. Here the Kerberos transferred the m-1 shares (ie. T_1 and T_2) only to the resource server and not the m^{th} share. This m^{th} share ($T_{3\text{-}7}$) is obtained from the client and then the resource server will generate the value of T by using Lagrange's polynomial. With the availability of the Kerberos SSO Token T, resources server can reissue the token to concern client when the Kerberos server is not available or Kerberos access token is expired. Once the entire process is over, then the client will get the new m^{th} share from the Kerberos KDC and it will discard the old token with the resource server. In the resource server end, Kerberos SSO will be get updated from the Cloud service provider access control information.

XI. PROPOSED MODEL COLLABORATIVE PKI (CPKI)

The proposed CPKI framework collaborates the Kerberos Centralized Authentication and Authorization service with decentralized GnuPG PKI to eliminate the issues which are identified in this paper. It is proposed as

a. In the Public cloud, Data Owner and Data User can choose their own trust by signing the public key in the web of trust model.

b. Cloud Service Provider (CSP) can decide their trust mechanism in the super host by using access control policy. CSP can generate the public key and can trust the user by signing their public key.

By introducing the user in the CSP public key, CSP will act as a central authority to allow the user to use the different application servers in the public cloud.

c. Web of trust model is protected with the kerberos server for authorizing the client request.

d. Super host extracts the fingerprint from the registered user's Public Key and passes the fingerprint into the KDC database. Kerberos SSO authorize the users based on the available fingerprint in the Public Cloud.

Whenever the user login into system node, GnuPG user process is started and Kerberos authentication is performed automatically, then the access policy from cloud service provider is downloaded in to client program through Kerberos server and this change the behavior of the user policies in the client system. The user can generate the private key and public key in the client system. This key pair is associated with unique ID called fingerprint. After the initial registration (Fig 2), the user will upload the master public key alone into superhost and keeps their master public and private key safely with them. The secret image is used to differentiate the same user in different client systems and kerberos identifies those users with their sub key. The user can generate the subkey pair which relates to the master key pair. The distribution of this sub public keys is done from the client system's kerberozied software by uploading into key servers (super host in modified CTES model).

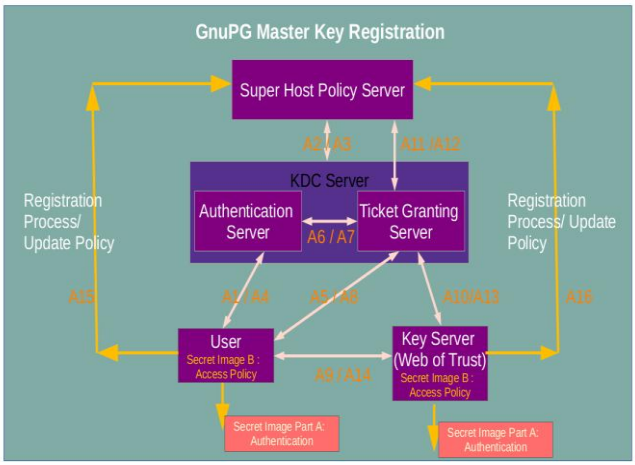


Fig 2 : GnuPG Master Key Registration

The client has the capability to work on Single-Sign-On with Application Server. For authenticating with Application Server, it simply provides the token generated from kerberos TGT server and get authorized to Application Server. This is applicable to all single sign on enabled cloud resources. The Application Server verifies the token with TGS server. If it matches, then the Application Server or any cloud resources will be available to provide the service to client. This proposed CPKI framework (Fig 3) provides security in end to end form with the security procedures of confidentiality, non-repudiation, authentication and integrity getting initiated at client end and applicable upto Application server. This end to end security procedures are applicable for web-based applications and for independent applications which are used to communicate from client to server or vice versa. Thus, GnuPG confirms that the data is arrived securely from sender by verifying with digital signature.

A. Trust Mechanism:

1. Whenever the user uploads their sub public key to super host (key server), Kerberos Single Sign-on validates the sub public key with the master public key's fingerprint. If it allows then only the user is authorized to upload the sub public key into key server.
2. The user is able to distribute the multiple sub keys in to different devices. The secret image identifies this sub key and Kerberos Single Sign-on validates it with the master public key's fingerprint. It helps the single user to get login in different devices.
3. The CSP can define the trust mechanism centrally in the super host and GnuPG user process validates the same with the use of Kerberos Single Sign-on. It means that the different user's public key can be introduced in the respective trusted public key certificate by CSP. Then the sender can send the message securely to the recipient with the help of trusted public key certificate.

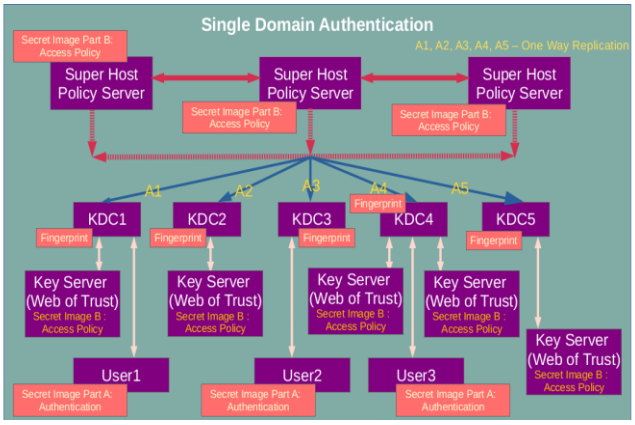


Fig 3: Single Domain Authentication

4. This CPKI model utilizes the PGP's Web of Trust model to upload or download the public key certificates by authorizing the CSP, Data Owner and Data Consumer (user) with Kerberos SSO in the public cloud. Thus, the CSP, Data Owner and Data Consumer (user) have rights based on the access policy from the superhost to introduce the other user's certificate in the PKI server. This access policy can define dynamically to introduce the certificate.
5. CPKI has the Unique ID based on the Domain Name System. It supports directly to send or receive the message with different domains. Thus, the unique name can be maintained under each domain.
6. If the certificate is compromised, then the transaction related to public and private certificate only can be removed and it will not affect the entire system. It is the user responsibility to recreate the private key and public key in the client node and upload the same into super host.
7. The authorized user can download another user's public certificate through kerberoized client software. It means that the Kerberos SSO validates the fingerprint of the downloading public key. This fingerprint can be obtainable from the secret image which is pushed from the superhost.

XII. PROPOSED ALGORITHM:

A. Generation of Kerberos SSO Token:

1. Generate the prime number.
2. Evaluates polynomial (coefficient tuple) at x.
3. Generate the random shamir pool to produce k shares with m minimum point.
4. Store the Kerberos token T and k share points in KDC.
5. Send the m-1 shares to the resource server.
6.Send the remaining shares from mth share to kth share into client.
7. Client will submit the mth share to resource server for gaining the resources.
8. Resource server will validate the mth share and retrieve the token T.
9. if Kerberos server is not available or Kerberos access token is expired, then the resource server will issue the rest of the token to complete the particular process.
10. If client finished its process with the particular resource server, it will discard the old token and request the new token from the Kerberos server.
11. In the resource server end, Kerberos SSO will be get updated from the Cloud service provider access control information.

XIII. COMPARISON OF THE PROPOSED COLLABORATIVE PKI

The proposed Collaborative PKI has the following benefits over the existing X.509 and GnuPG based model (Fig 4).

Comparison of the Proposed Collaborative PKI (Fig 4)

Features/Benefits	Proposed CPKI	X.509 PKI	PGP
Certificate Format	It contains self signature and can also obtain multiple signatures.	It supports only a single digital certificate to attest to the key.	It contains self signature and can also obtain multiple signatures.
Public Key	It has different labels which identify the user in multiple ways.	It has only a single name for key owner.	It has different labels which identify the user in multiple ways.
Certificate introducer	It can use digital signature as the introducer.	Certification Authority (CA) is the certificate's introducer.	It can use digital signature as the introducer.
Chain of trust	A PGP user public key certificate can also validate another PGP user's public key certificate. Moreover, such a certificate is only valid to another user if another party recognizes the validator as a trusted introducer.	When any user signs another user's key, then the user becomes an introducer of that key. With the flow of this process, it establishes a chain of trust, so any user can act as a certifying authority (CA).	A PGP user public key certificate can also validate another PGP user's public key certificate. Moreover, such a certificate is only valid to another user if another party recognizes the validator as a trusted introducer.
Responsiblity of Key Management	PGP user is the one that manages keys. In the Public Cloud, KDC checks the authenticity of all PGP certificates with the master finger print and sign the good ones.	X.509 CA manage the keys	PGP user is the one that manages keys. In an organization which is using PGP certificates, the job of the Central Authority is to check the authenticity of all PGP certificates and then to sign the good ones.
Issue of Certificates	PGP user issues the certificates. Web of trust model is protected with the kerberos server for authorizing the client request.	In an organization using a PKI with X.509 certificates, the job of the RAs is to approve certificate requests and the job of the CA is to issue certificates to users.	PGP user issues the certificates.
Revocation procedure	PGP certificates provide the added feature that user can revoke his or her entire certificate if user feels that the certificate has been compromised. The certificate's owner can revoke a PGP certificate.	In X.509 certificates, the revoked signature is almost the same as a revoked certificate given that the only signature on the certificate is the one that made it valid in the first place i.e. the signature of the CA.	PGP certificates provide the added feature that user can revoke his or her entire certificate if user feels that the certificate has been compromised. The certificate's owner can revoke a PGP certificate.
Responsiblity of Revocation certificate	The certificate's owner can revoke a PGP certificate.	Only the certificate's issuer can revoke an X.509 certificate. Communication of revoked X.509 certificates is most commonly achieved via CRL, which is published by the CA.	The certificate's owner or revoker can revoke a PGP certificate.
Syntactic	PGP allows certificates to be in stack form	X.509 the certificates are linked one to another just as in an one-way linked-list	PGP allows certificates to be in stack form
Semantic	PGP allows an association between keys and real-world persons by web-of-trust rules, and not by transitive trust rules	X.509 it binds keys to names and accepts transitive trust	PGP allows an association between keys and real-world persons by web-of-trust rules, and not by transitive trust rules
Centralized Authentication	Web of trust model is protected with the kerberos server for authorizing the client request. CSP will act as a central authority to allow the user to use the different application servers in the public cloud.	Certificte Authority is available for authenticate the certificates. It is centralized PKI.	It is decentralized PKI and does not depend upon central authentication.
Single Sign On	Kerberos Sigle sign on is available. Kerberos Single Sign-on validates the sub public key with the master public key's fingerprint. If it allows then only the user is authorized to upload their sub public key into key server.	SSO is not available.	SSO is not available.
Access Control Poicy	Access Control policy can be achived directly.	Access control policy can be achived with directory service only.	Aaccess control policy is not available.

XIV. RESULT

The proposed algorithm is implemented by using Python Language version 2.7.17 in the Lenovo Ideapad 130 core i3 7th Gen, 4GB RAM and using the prime number 170141183460469231731687303715884105727. Table 1 shows the generating of SSO token with different values of m share and k shares from the SSO Token value of 170141183460469231731687303715884105727.

Table 1 : Generation of Kerberos SSO Tokens.

Coefficient Value X	Secret Share M Value	Secret Share K Value	SSO Token
1	3	7	12870264348783921055 184757172822535805 3L
2	3	7	281774788949411855509 33413130363720439L
3	3	7	115189881039680093521 411655193873529398L
4	3	7	49457483001117470999 907690486986573476L
5	3	7	112146823972254971810 8822725586958400L
6	3	7	1403230202159645614077 02355625558789897L
7	3	7	1267797720089050426053 1 3681755133856513L

Here the Kerberos transferred only two shares (ie. m-1 shares) into the resource server and the remaining four shares will be obtained by clients. Clients will submit these tokens to get access the resources in the resource server. Then the resource server will generate the value of T by using Lagrange's polynomial. With the availability of the Kerberos SSO Token T, resources server can reissue the token to concern client when the Kerberos server is not available or Kerberos access token is expired.

XV. CONCLUSION

Kerberos authentication database at KDC maintains the public key fingerprints and Kerberos SSO tokens of all the users in the public cloud. Public key certificate is available in the web of trust PKI server. Superhost maintains the record of all clients and Application Servers including web of trust PKI server and provides the access service to the authenticated client. GnuPG fingerprints can be used for allowing client to upload or download the GnuPG subkeys into the PKI Server. The proposed CPKI framework collaborates the Kerberos Centralized Authentication and Authorization service with decentralized GnuPG PKI to eliminate the issues which are identified in this paper. This proposed Collaborative PKI will be considered as a novel step towards the use of both the technology of Kerberos and GnuPG.

REFERENCES

1. Ashok Kumar J & Gopinath Ganapathy. (2017). An Enhanced CTES Design for Authentication and Authorization to Cloud Services and Resources. International Journal of Applied Engineering Research, 12(24), 15693-15698.
2. Ashok Kumar J & Gopinath Ganapathy. (2017). A Modified Approach for Kerberos Authentication Protocol with Secret Image by using Visual Cryptography. International Journal of Applied Engineering Research, 12(21), 11218-11223.
3. William stallings (2006). Cryptography and network security principles and practices. (4th ed ed.). Pearson Prentice Hall.
4. Kamarudin shafinah & Mohammad mohd ikram (2011). File Security based on Pretty Good Privacy (PGP) Conce. Computer and Information Science, 4(4), 10-28.
5. Michael louie loria. (2014). Pretty Good Privacy. Retrieved 14 Novem ber, 2019, from http://slidedeck.io/michaellouieloria/pgp
6. Xiaowei Gao, Zemin Jiang, Rui Jiang. (2012). A Novel Data Access Scheme in Cloud Computing. 2nd International Conference on Computer and Information Application (ICCIA 2012).pp 0124-0127.
7. DonArmstrong. (2018). https://wiki.debian.org/Subkeys
8. "Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile, rfc 3280," 2002
9. Xiaowei Gao, Zemin Jiang, Rui Jiang. (2012). A Novel Data Access Scheme in Cloud Computing. 2nd International Conference on Computer and Information Application (ICCIA 2012).pp 0124-0127.
10. Alfarez Abdul-Rahman. The PGP Trust Model. https://pdfs.semanticscholar.org/e9aa/5d8032c1d925ea6a02dd3be93f42e831c965.pdf
11. Adi Shamir, Massachusetts Institute of Technology. https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf