IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 6, June 2015.
www.ijiset.com
ISSN 2348 – 7968

# QOS for Performance Accelerators and PKI in Secure Cloud

**M. Subrahmanya Sarma[1], Y Srinivas [2], M. Abhi Ram [3]**

[1]Senior Manager, IBM , Bangalore, abhiswaaru@gmail.com,

[2]Professor , Department of IT GITAM University ,sriteja.y@gmail.com,

[3]B. Tech (C.L), GITAM University, ramabhisharma2@gmail.com

**Abstract:** Cloud adoption is getting increased significantly, could users are looking for more quality of services to manage the security in their cloud images. In this paper we suggest additional quality of services to enhance the performance of security operations. Public key infrastructure has significant role to play especially in managing the SSL connectivity between two end points. We also suggest the cloud service providers to supply the PKI Infrastructure with OCSP protocol implementations to the cloud users as a quality of services. Experimentation results are attached in this paper.

**1. Introduction**: Cloud end user expectations are increased with increase of penetration in Cloud. Cloud service providers should provide more quality of services for optimizing the performance of cloud end user security operations. PKI services should be provided as Quality of Services by the service provider for efficient Key Management and for digital certificates covering SSL server and SSL client certificates. In this paper we proposed a Quality of Service model (QOS) to extend the entire security framework as QOS. We have also proposed performance accelerators to enhance the performance of security operations especially the decryption of files in Security Wallet (scheme proposed in [18]). Section 3 of the paper describes proposed QOS model in cloud. Section 4 covers the experimental results and concluding section 5 concludes this paper.

**Index Terms**: Secure Cloud, QOS, Performance Accelerators and PKI

## 2. Related Work

Srinivas Y and Subrahmanya Sarma [6] elaborated the various security issues and mechanisms in cloud computing. Privacy issues are of highest concern to the user community, cloud users are unaware about the information pertaining to the actual storage area of data and in which data center the information is stored. To address the privacy issues, cloud providers should provide tools for encryption and decryption of the cloud images [7] [8]. Integrity issues are of next major concern to the user community, where in cloud service providers should provide tools to digitally sign and verify the information on the cloud images[9][10][11] . Cloud service providers should ensure only authorized users to access the cloud resources for which they are entitled for. This can be achieved by using IAM (Identity and Access Management Solutions). Cloud service providers should ensure the involvement of the cloud users in cloud transactions. This can be achieved via Digital signatures. The following table summarizes the security issues and the mechanisms.

ISSN 2348 – 7968

| Security Issues | Mechanism |
|---|---|
| Cloud Confidentiality | Encryption |
| Cloud Integrity | Digital signatures |
| Cloud Authenticity | Digital signatures and Access Management via IDaas |
| Cloud Non Repudiation | Digital signatures |

Srinivas Y, Subrahmanya Sarma and Abhi Ram M compared [17] RSA and ECC Public key algorithms and concluded RSA is a preferred algorithm when compared with ECC for cloud implementations.

Srinivas Y, Subrahmanya Sarma and Abhi Ram M [18] , introduced quality of Services for public key encryption , symmetric encryption and Digital signatures. They classified the information to be stored in the Cloud and suggested to organize the information in a structured form called Wallet.

## 3. **Proposed Model of Cloud with Quality of Services.**

In the secure wallet model proposed [18], all the sensitive information is encrypted and stored in wallet. As the usage of wallet and cloud image is increased , at some point of time , the number of files in the wallet gets increased . Moreover the cloud users need not require all the files to be decrypted and made available to the cloud user. We propose to add file filters as quality of services by cloud service provider so that the users decrypt only the required files between two specific dates without decrypting all the files. If users needs files outside this time boundary, required files should be decrypted separately. This approach decrypts only needed files and improve the systems performance, reduce the cost and optimize the resource utilization. In cloud based developments, cloud users are in need of SSL server and SSL client certificates to provide SSL connectivity between two end points. Cloud service providers should provide PKI as a QOS to the end users. Cloud services providers can leverage leading PKI service providers like Verisign or Entrust as CA provider or any open source CA like EJBCA or OpenSSL. Cloud service provider should provide OCSP ( Online Certificate Status Protocol) implementations for immediate response on certificate status. Please refer to Fig. one for the proposed architecture.

ISSN 2348 – 7968

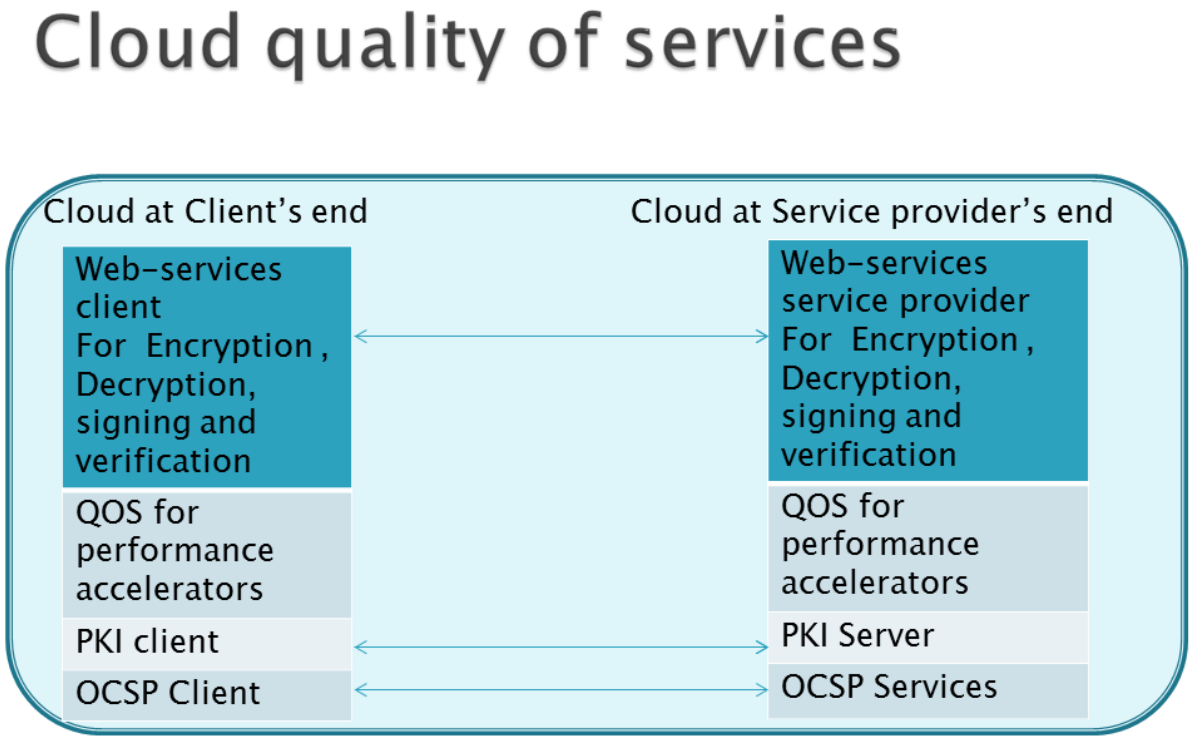



Fig. One

### 3.1. **QOS for Performance Accelators**.

Performance is one of the key considerations in cloud deployments. It attributes directly the costing for the end users as it impacts the network traffic and bandwidth. We propose a performance filter , where in instead of decrypting all the files in the secure wallet , only the files , which are need of the hour gets decrypted. This approach would result in a lot of savings of cost for decrypting of unused files and also processor capability. This file filter should be applied to choose the files which are required between the two dates.

**Procedure File Filter (** File directory. Date start date , Date end date )

/* this procedure applies the file filter and returns the list of files to be decrypted*/

Begin

File[] files = directory.listFiles();

For ( File file :files)

Begin.

Date lostmodifed = new Date ( file.lostModified());

ISSN 2348 – 7968

If (lostmodifed ) >=startDate ) and (lostmodifed <=enddate)

Add the filename to the list_ of_files_ to _be_decrypted

End

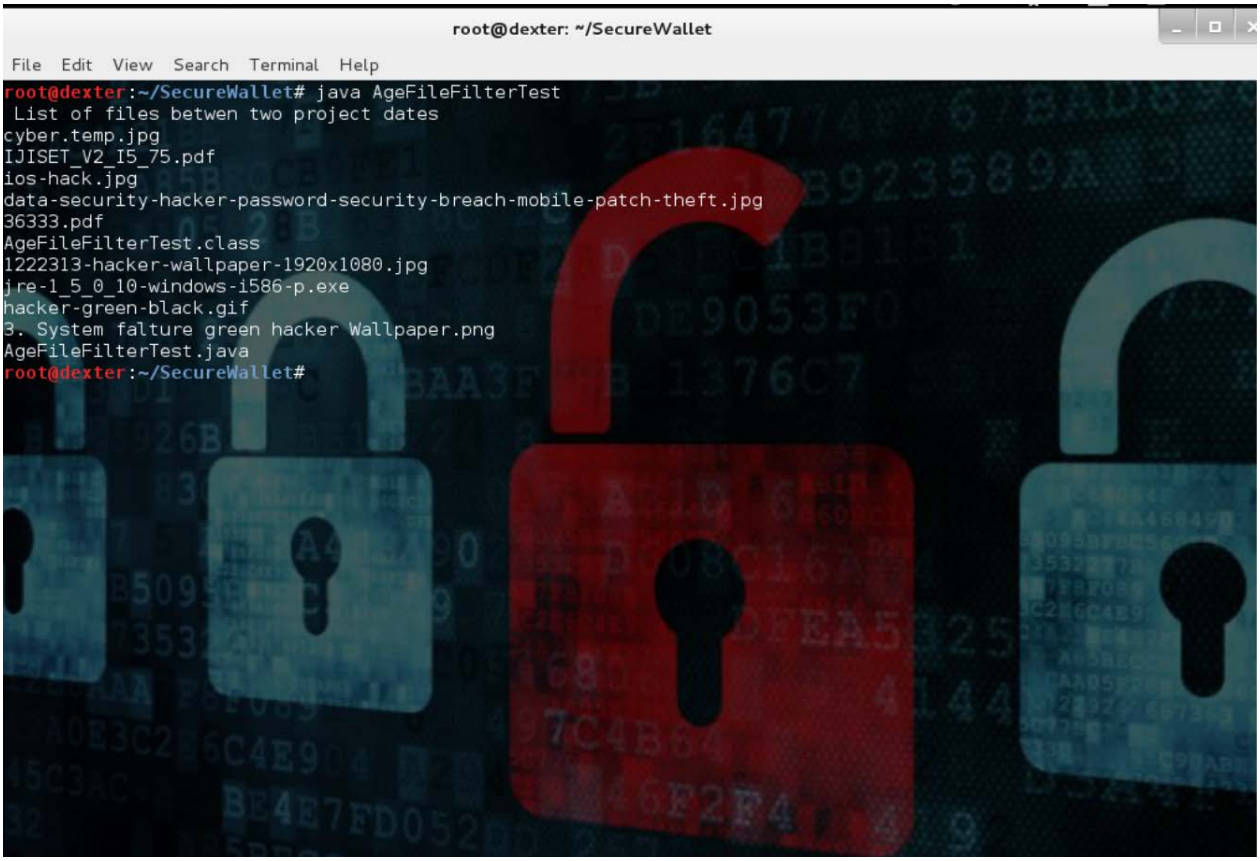
End.

3.2 **QOS for PKI Services:** Public Key Infrastructure (PKI) is an Infrastructure [19] designed to manage end user keys via digital certificates. Digital certificates binds subject (users) with a public key. PKI provide unique way to secure many applications covering email, SSL and VPN. PKI enables digital signatures and encryption to provide PAIN (Privacy, Authenticity, Integrity and Non Repudiation). It prevents the threats due to sharing of the keys and passwords over the wire. PKI enables the trust between two or more parties (possibly from different organizations or nations) without prior knowledge of each other. PKI uses public key cryptography, keys are generated using industry standard algorithms (RSA) by certificate authorities. Private Key is shared to requesting party (end users) and public keys are kept open to the public as part of certificate. These certificates are stored in LDAP V3 compliant directory servers. Certificate Authority manages the complete life cycle of certificates covering creation, revocation, suspension and re-instantiation. Certificate authorities also publish periodic certificate revocation lists and also online status of certificates via OCSP protocol implementation. In the larger deployments like cloud, PKI implementation, OCSP are bundled in one place to cover the certificate life cycle Management and its status response. Cloud users needs digital certificates for key management, SSL configuration and SSL Client Authentication. We propose PKI infrastructure should be supplied as Quality of Service by the Service provider. We have done experimentation with OpenSSL open source PKI. However cloud service providers can ship any of the open source PKI implementations like EJBCA or partner with leading PKI service providers covering Verisign and Entrust for the PKI deployments.

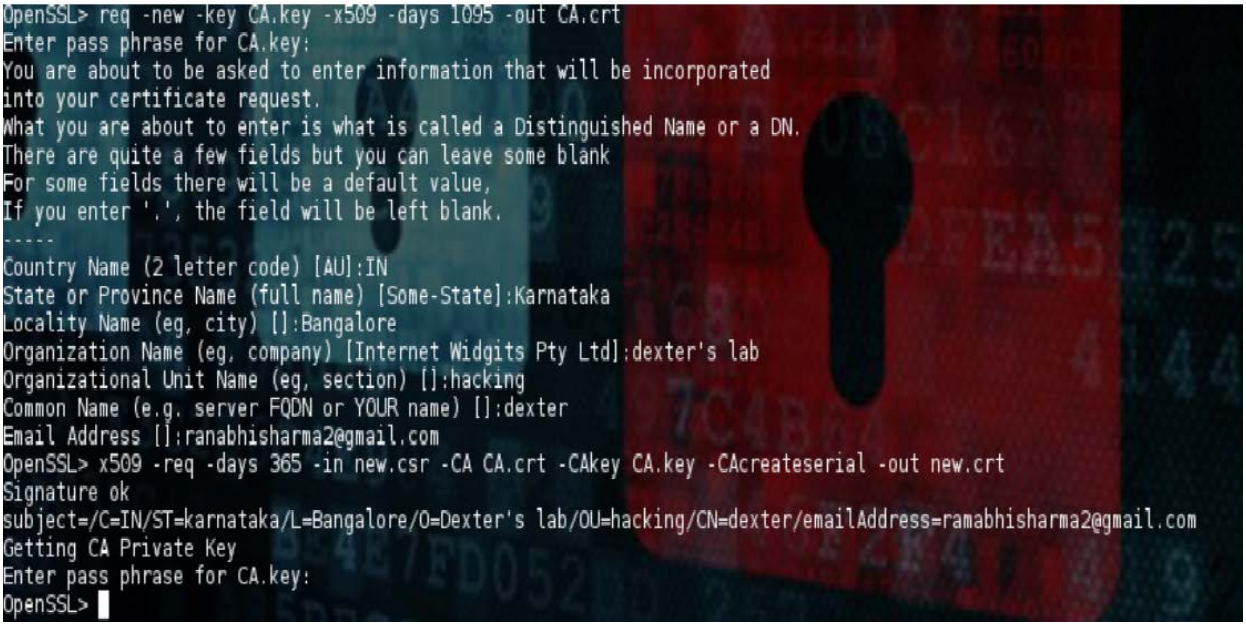
## 4. **Experimentation Results**

4.1 QOS for performance accelerators: We have implemented the Filefileter accelerators in java.

ISSN 2348 – 7968




### 4.2 QOS for Public Key infrastructure: We have implemented PKI using OpenSSL open source library



ISSN 2348 – 7968

5. Conclusion

End users expectations are increased with increasing traction of the cloud. Cloud service provider should extend more QOS for the cloud users to manage their end to end security . We propose a new QOS model to extend performance acclerators and PKI as quality of services. Further work can be carried out to add more quality of services to this model to improve the end user experience in managing the end to end security in the cloud.

## 6. **References**

[1]. Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. OReilly Media, Inc., Sebastopol, CA

[2]. Li W, Ping L (2009) Trust model to enhance Security and interoperability of Cloud environment, In Proceedings of the 1st International conference on Cloud Computing , Springer Berlin Heidelberg, Beijing, China, pp 69–79

[3]. Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press

[4]. Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0. Available: https://cloudsecurityalliance.org/research/top-threats

[5].Dahbur K, Mohammad B, Tarakji AB (2011) A survey of risks, threats and vulnerabilities in Cloud Computing. In: Proceedings of the 2011, International conference on intelligent semantic Web-services and applications. Amman, Jordan, pp 1–6

[6]. Dr Ysrinivas , Subrahmanya Sarma, Security issues in cloud computing , (GJCSIT) Global Journal of Computer Science and Information Technology, Vol. 1 (1), 2014, 43-46

[7]. Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing. In Proceedings of the 2010 International conference on Security and Management SAM'

[8].Grobauer B, Walloschek T, Stocker E (2011) Understanding Cloud Computing vulnerabilities. IEEE Security Privacy 9(2):50–57

[9] Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security: Challenges and solutions. In the 7th International Conference on Informatics and systems (INFOS), Potsdam, Germany. IEEE Computer Society, Washington, DC, USA, pp 1–8

[10] Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In IEEE International Carnahan Conference on Security Technology (ICCST), KS,USA. IEEE Computer Society, Washington, DC, USA, pp 35–41

[11].Garfinkel T, Rosenblum M (2005) When virtual is harder than real: Security challenges in virtual machine based computing environments. In Proceedings of the 10th conference on Hot Topics in Operating Systems, SantaFe, NM. volume 10. USENIX Association Berkeley, CA, USA, pp 227–22

[12]https://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/

[13].http://vanilla47.com/PDFs/Cryptography/Miscellenea/Eliptic%20Curve%20Cryptography/A_tutorial_of_elliptic_curve_cryptography.pdf

[14].http://en.wikipedia.org/wiki/ECC_patents.

[15]. http://www.ijser.org/researchpaper/Performance-Based-Comparison-Study-of-RSA-and-Elliptic-Curve-Cryptography.pdf

[16] Miland Mathur , Aysuh Kesharvani , COMPARISON BETWEEN DES , 3DES , RC2 , RC6 , BLOWFISH AND AES Proceedings of National Conference on New Horizons in IT - NCNHIT 2013.

[17] Dr Ysrinivas , Subrahmanya Sarma, Best fit algorithms for ensuring security in cloud environments – A Compartive study of RSA and ECC. International Journal of Modern computer science and Applications. ISSN:2321-2632( Online) , Volume no3 Issue No 1. January 2015.

[18] DR . Y Srinivas , M Subrahmanya Sarma , M Abhiram , Securing Cloud with Quality of Services , IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 5, May 2015. ISSN 2348 – 7968

[19] http://www.ietf.org/rfc/rfc2459.txt