Journal of Theoretical and Applied Information Technology
30th November 2019. Vol.97. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCING DATA SECURITY IN CLOUD COMPUTING USING PUBLIC KEY INFRASTRUCTURE

[1]OUADIA ZIBOUH, [2]ANOUAR DALLI, [3]HILAL DRISSI

[1,3]Laboratory of Systems Analysis, Information Processing and Integrated Management,

High School of Technology EST-Salé, Mohammed V University Rabat, Morocco

[2]Department of Telecommunications and Networks Engineering,

National School of Applied Sciences-Safi, Cadi Ayyad University Marrakesh, Morocco

E-mail: [1]ouadia.zibouh@gmail.com, [2]anouar_dalli@yahoo.fr, [3]hilaldrissi@gmail.com

ABSTRACT

Cloud computing is an emerging computing paradigm which is perceived as the technological innovation that will transform future investments in information technology. This new technology is a growing trendy platform that is gaining an expanding interest, since it provides several benefits to its users by offering efficient architectures that support the transmission, storage, and intensive computing of data. Meanwhile, the rapid growth of cloud computing increases the vulnerability of unauthorized disclosure and unauthorized modification. Cloud security is the major hurdle in wide adoption of cloud computing. Hence, there is a need of an appropriate security and privacy solution that provides all security services. This paper proposes and implements the public key infrastructure cryptography scheme combined with IPSec VPN to strengthen security and privacy in the cloud environment. The proposed architecture based on certificate authority that provides the service of binding X509 certificate with user's identity, and which ensures the protection of critical data stored in cloud.

Keywords: *Cloud Computing, Cloud Security, Hash value, IPSec VPN, Public Key Infrastructure, X.509*

1. INTRODUCTION

Cloud computing has become a prominent paradigm of computing and IT service delivery. It is an information technology type which is used to store, manage and process data on remote site. Nowadays, cloud computing is one of the most enticing technologies that offers potential benefits to users by delivering IT capabilities (software, platforms, hardware) as a service request, scalable and elastic [1]. However, the data security continues to be one of the top concerns for cloud computing that slows its widespread adoption. According to the recently Verizon's annual Data Breach Investigations Report that provides analysis of information security incidents, with a specific focus on data breaches, the number of security incidents has risen about 11,000 and data braches by 280 compared to previous year's report. This survey has categorized these security incidents and data breaches into a series of patterns that share enough commonalities as shown in the figures 1 and 2 [2]. Last year's report details the continued prevalence of ransomware and the impact on organizations as they face a rising number of attacks. One example of this was WannaCry, a ransomware that infected hundreds of thousands of victims using recently released Shadow Brokers exploits DoublePulsar and EternalBlue. This attack caused major headaches and confusion across the globe. Security continues to be the critical issue and remains a key decision factor for migration of resources to the cloud provider [3]. Several existing security solutions implement different types of security features that implies a limitation of performance, and also require a high computational power or memory or high bandwidth. Hence, storing sensitive data in the cloud without putting in place appropriate security and privacy solution will cause some critical data security problems to its

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

users. This security framework should be able to cover all aspects of security. It should incorporate confidentiality, integrity, authentication, and non-repudiation. These aspects are supported by a number of security solutions. One of them is a Public Key Infrastructure (PKI). It is a very powerful technology that provide security services to users for establishing secured electronic communications like email, web service, virtual private networks, and authentication systems. In PKI, a trusted third party called certificate authority (CA) issues and signs the digital certificates by using its private key. A certificate is used to bind an entity's identity information with the corresponding public key.

The main objective of this research is to implement a security model on cloud infrastructure which provides high security level and suitable for the business applications. We proposed the implementation of Public Key Infrastructure scheme with IPSec VPN on a national network (between different branches of a public institution in Morocco) to ensure data exchange in a secure way.

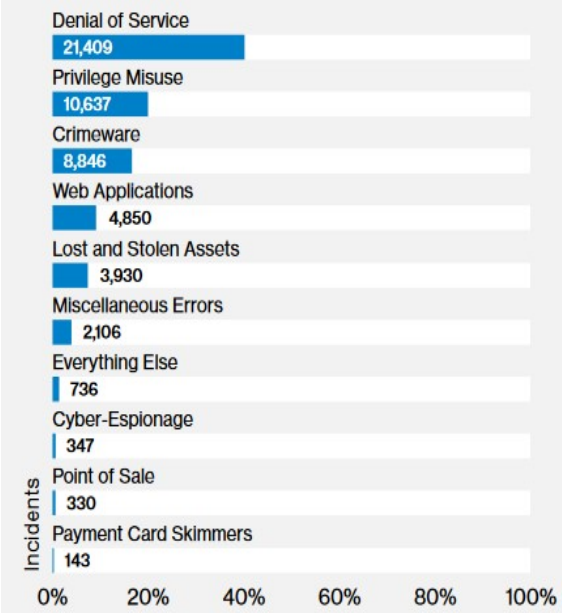

Figure 1: Percentage and count of incidents per pattern (n=53,308)

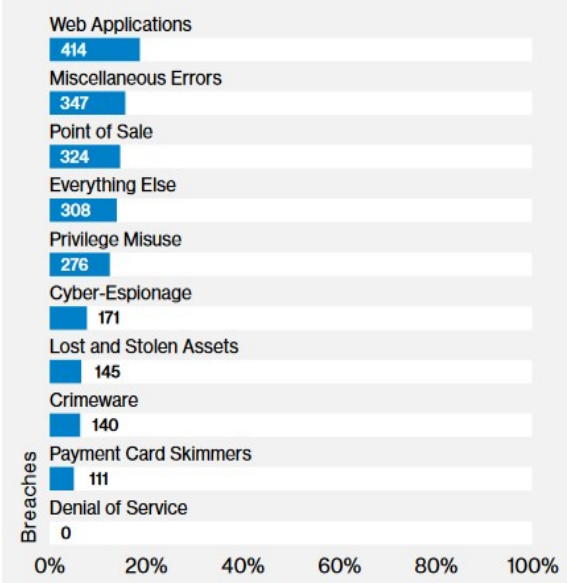

Figure 2: Percentage and count of breaches per pattern (n=2,216)

The rest of the paper is organized in the following sections. Section 2 presents a background knowledge of PKI technology, including PKI services, PKI components, digital signature and X509 certificates. Section 3 describes the proposed approach to provide high security level to cloud computing by ensuring the safety and privacy of information exchanged over various network infrastructures. Evaluation of proposed approach is discussed in section 4. Finally, the work is put in a nutshell by a conclusion in Section 5.

2. PUBLIC KEY INFRASTRUCTURE

Public key infrastructure has become widespread as a modern way to protect users, networks, data and critical business systems. This system is replacing traditional symmetric system due to its advance protection shield against security attacks. It enables integration of various services that are related to cryptography in order to protect sensitive data during transmission. PKI is a framework that consists of encryption, key exchange, digital signatures, and digital certificates [4]. It contains the set of roles, policies, and procedures needed to generate, manage, distribute, renew, store, and revoke digital certificates to provide ultimate security [5].

2.1 Services of PKI

A Public Key Infrastructure enables users of a basically unsecure network to ensure secure electronic data exchange through the use of a public

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and a private cryptographic key pair provided by a trusted authority [6]. The aim of PKI is to provide these major security services:

- Confidentiality: It is a mechanism in which original contents of the message is encrypted by cryptographic algorithms. It is the process through which it is ensured that data will only be decrypted by only authorized user [7]. The data is not made available or disclosed to unauthorized individuals, entities, or processes.
- Integrity: It is the assurance that maintains the consistency, accuracy, and trustworthiness of data over its entire life cycle. It ensures that data transmitted from source is exactly the same that has been received at destination [8]. PKI validates that all the outputs are equivalent to the inputs and any alter of the data can be immediately detected and prevented by applying hash function. The value of hash function should be same on the sender and receiver side[9].
- Authentication: It is the process that ensures and confirms a user's identity. The Public Key Infrastructure authentication method uses digital certificates to prove correctness of source identity[10].
- Non-repudiation: It is a method of guaranteeing message transmission between parties via digital signature and/or encryption. It means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message, so neither can later deny having processed the data [11].

2.2 Components of PKI

The main components of PKI infrastructure are:

- Certification Authority (CA): It is the trusted third party that digitally signed certificate. This component is directly responsible for the creation of certificate, issue of certificate, and the management of public-key certificates that are in use for a PKI[12].
- Registration Authority: It is an optional component that performs multiple administrative tasks from CA. It is responsible for accepting requests for digital certificates and authenticating the entity making the request[13].
- Repository: It is a database which is easily accessible to all the users of the PKI system. It is used to store and distribute certificates and revocation of certificates through the process of Certificate Revocation Lists (CRL)[14].
- Archives: It is used to store all the information that is archived by the CA such as documents and revoked certificates related to old or inactive certificates that can be used to settle future conflicts[15]. The data modification in the archives is not recorded when the archive process is going on[14].
- Certificates: are electronic documents issued and signed by a certification authority (CA) that binds the physical identity of an entity (user, organization or computer) to their public key. By being signed by a recognized and trustworthy authority a certificate provides the guarantee that a specific public key belongs to an entity [16]. It contains public key, the entity information (such as name, postal address, E-mail etc.), validity period and the CA's own digital signature.

2.3 Digital Signature

A digital signature is a mechanism of authentication to a message which enables clients to validate the issuer's identity and prevents the message being altered or modified in any way while traversing the network.

Using a digital signature means applying the sender's private key to the message, or document, or to the message digest. If the signature can be decrypted with the sender's associated public key, it will establish the identity of the owner and verify that the message has not been altered since it was signed [17].

A digital signature performs a hashing algorithm on the data to be encrypted, the outcome of this is a computational value based on the contents of the data[18]. This hash value is known as the message digest. The value of the hash is unique to the hashed data[19]. Any change in the original data, even changing or deleting a single character, results in a large change in the message digest produced[20]. This attribute enables others to validate the integrity of the data by using the signer's public key to decrypt the hash. By performing the same hash function on the decrypted data, the message digest can be obtained by the receiver and she can compare it with the one sent by the sender to ensure that

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the contents are not altered, hence guaranteeing integrity and non-repudiation [9].

For instance, if we suppose that the sender wants to sign a message digitally to the receiver, the sender will encrypt the message digest with his private key to create a digital signature. He will encrypt the document using receiver's public key and sign it using his digital signature as illustrated in the figure 3. This ensures that the receiver can verify that the document is sent by the claimed sender, by verifying the digital signature using the sender's public key. The receiver can also verify that the document is not altered and arrived intact by validating the message digest, and also can open the encrypted document using his private key.

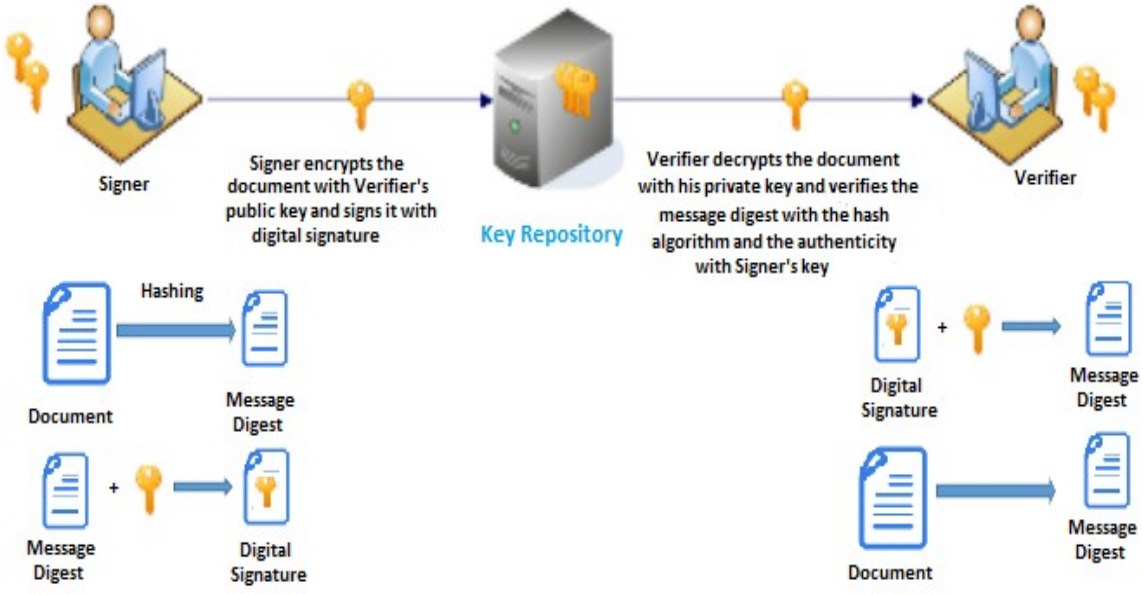

Figure 3: Digital signature

2.4 Overview of X509 Certificates

Digital certificates are signed data structures that bind attributes of an entity with its corresponding public key. They are issued to a person, system, or an organization by a competent authority called a Certificate Authority (CA) after verifying the credentials of the entity. In PKI, digital certificates are used for authenticity verification of an entity.

One of the important and most universally PKI standards pertaining to digital certificates is X.509. It is a standard published by the International Telecommunication Union (ITU) that specifies the standard format for digital certificates [21]. The digital signature is generated by the process of X.509 encryption algorithm which is used to take input of various contents of the X.509 digital certificate accompanied with a private key [14]. This digital signature is appended and associated with a X.509 certificate. Moreover, all digital signatures along with their certificates are validated to the receiver of the messages which possesses the sender public key corresponding to private key used for generation of digital signature inside the X.509 certificate process [14]. There are three different versions of X.509. The version number of the certificate specifies the fields and formatting of the certificate which indicates what data the certificate must include and therefore how it is to be interpreted by the applications which make use of it. The most recent version is 3 and this is the most used version [22]. X.509 version 3 offers significant improvements over Version 1 and Version 2 through the addition of optional extensions that provide additional functionality and features to the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

certificate and which can create bindings for information about keys, subject identification, policy and certificate path constraints. These extensions provide us with a framework for adding optional elements for application distribution and control [23]. Figure 4 illustrates the standard format of all versions of x.509 certificate. Standard information in an X.509 certificate includes:

- Version: It specifies the version number of the encoded certificate (which indicates what data the certificate must include).
- Serial Number: It is a unique number assigned by the certification authority to each certificate.
- Signature Algorithm Identifier: It identifies the algorithm used by the CA to sign the certificate.
- Issuer Name: It provides a distinguished name for the CA that has signed and issued the certificate.
- Validity: It Specifies the time interval during which the certificate is valid.
- Subject Name: It describes the name of the entity to whom certificate is assigned.
- Subject public key information: It determines the public key algorithm, type and length associated with the certificate.
- Subject/Issuer Unique Identifier: It is an optional field. It is used to handle the possibility of reuse of subject and/or issuer names over time.
- Extensions: This field is only available in version 3 certificates. It provides methods for associating additional attributes for optional use by public key infrastructures.

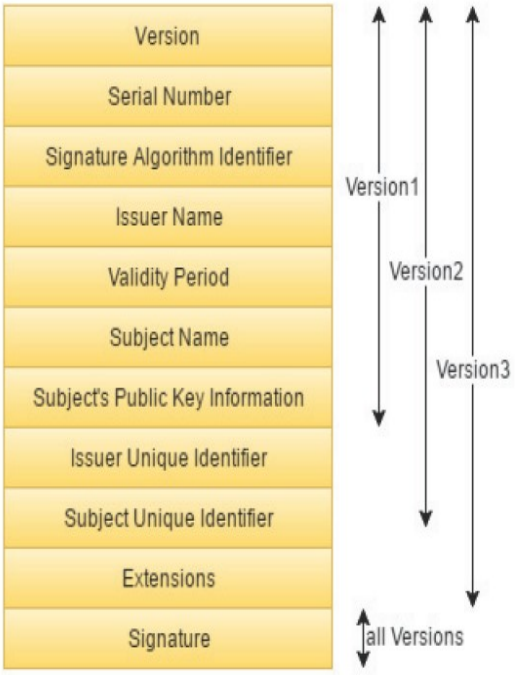

Figure 4: Standard format of X.509 certificate[24]

Certificate validation is a key part of certificate usage. The validation process performs a series of checks on different parts of the X509 certificate (illustrated in Figure 5) : trust check, digital signature check, time validity check, revocation check, and formatting check [23]. The X509 certificate is considered valid only after passing all these checks with success.

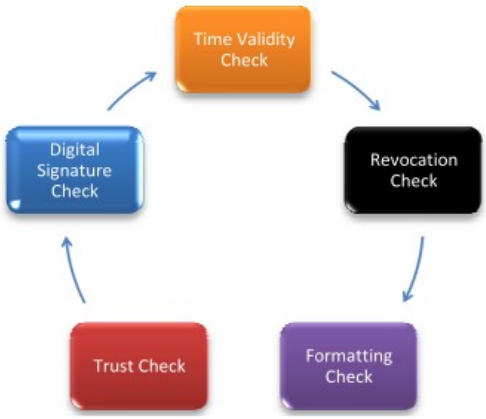

Figure 5: X509 Certificate Checks[23]

3. PROPOSED APPROACH

In order to achieve secure communication and avail offered services of cloud through secure infrastructure, our

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

proposed approach consists in designing and implementing the public key infrastructure in private cloud. This scheme was implemented on a national network between different branches of a public institution in Morocco. The target infrastructure of our approach is illustrated in the figure 6. All remote users from different branches can securely communicate with production server through VPN tunnels and their access is authenticated through organization firewalls. It is an another security layer that has been established to secure the traffic over un-secure channels. In our proposed secured architecture, after VPN connection establishment, the user should be initially authenticated to CA SSL server to ensure that the user possesses the valid X509 certificate. This server is responsible to issue and hold certificates to users in cloud environment. After a successful check of the user certificate, he can use his identity and password to login to the deployed applications in the private cloud of the public institution.

Our experimental environment consists of a physical server HP proliant DL320e G8 equipped with 4 Intel Xeon E3-1220v2 3.1 GHz, 16GB of RAM, and 2x1TB 12G SAS 7.2K rpm SFF. As our virtualization technology, we used VMware vSphere 5 (ESXi-5.0) that was installed directly on the physical server and deploying two VMs as follows: the first VM is equipped with Ubuntu Server 14.04 LTS, enabling the TLS/SSL module for its services and it plays the role of CA server SSL. The second VM is equipped with Ubuntu Server 14.04 LTS and it plays the role of reverse proxy server.

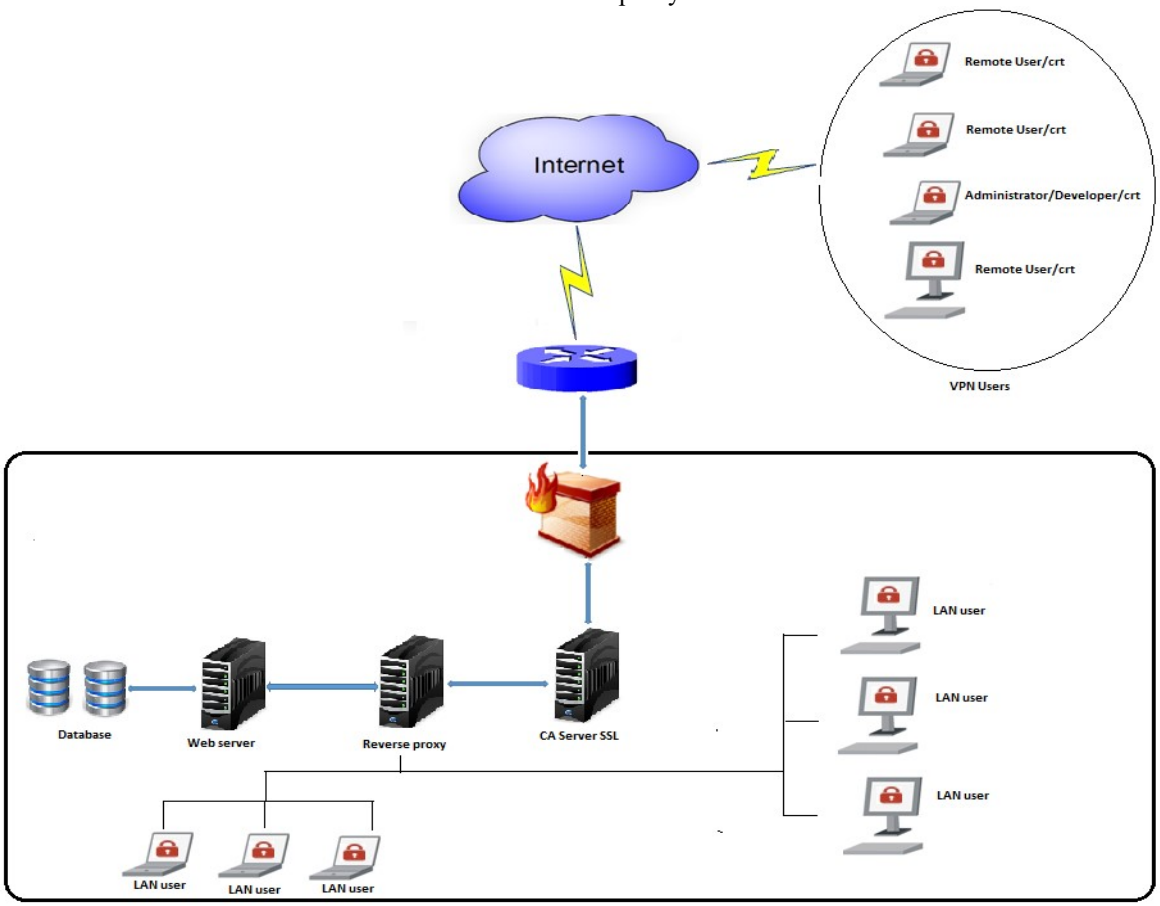

Figure 6: Proposed approach architecture

The creation of certificates can be made directly in the authentication server by command line. It also exists graphics tools very intuitive that can replace the command line. The tool we chose for SSL certificate management is X Certificate and key

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

management XCA (Figure 7). It is one of the most popular PKI libraries which is written in C language and available under the BSD public license with no restrictions on use. XCA is an application for creating and managing X.509 certificates, certificate requests, RSA, DSA and EC private keys, Smartcards and Certificate revocation lists(CRLs). XCA supports several formats like PKCS #7, PKCS, PKCS #11, PKCS #12. In addition, XCA also supports common cryptography algorithms such as RSA, DSA and ECDSA [25].

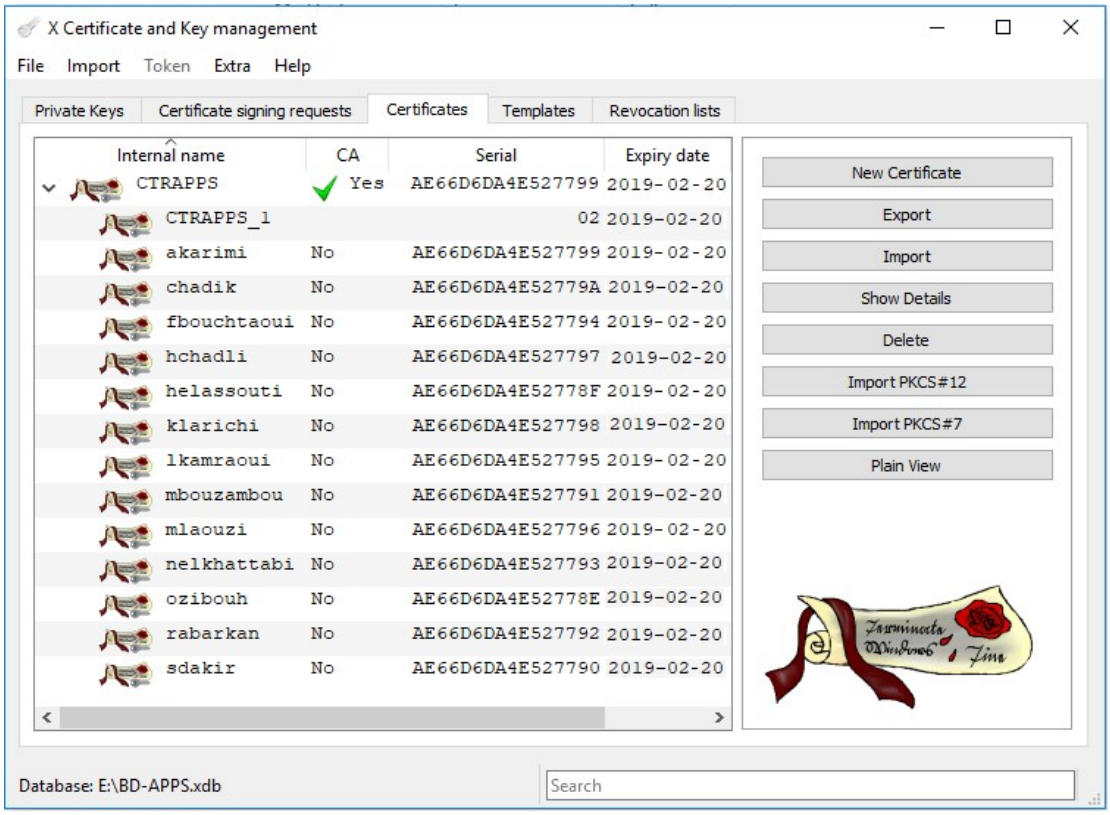

Figure 7: XCA interface

The hash algorithm we used by default to generate the hash values is SHA 512 which is widely considered for use in data integrity assurance and data origin authentication security services. In our model, we propose a creation of a private key associated to a public key using RSA algorithm with key size 4096 bits as shown in the figure 8.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

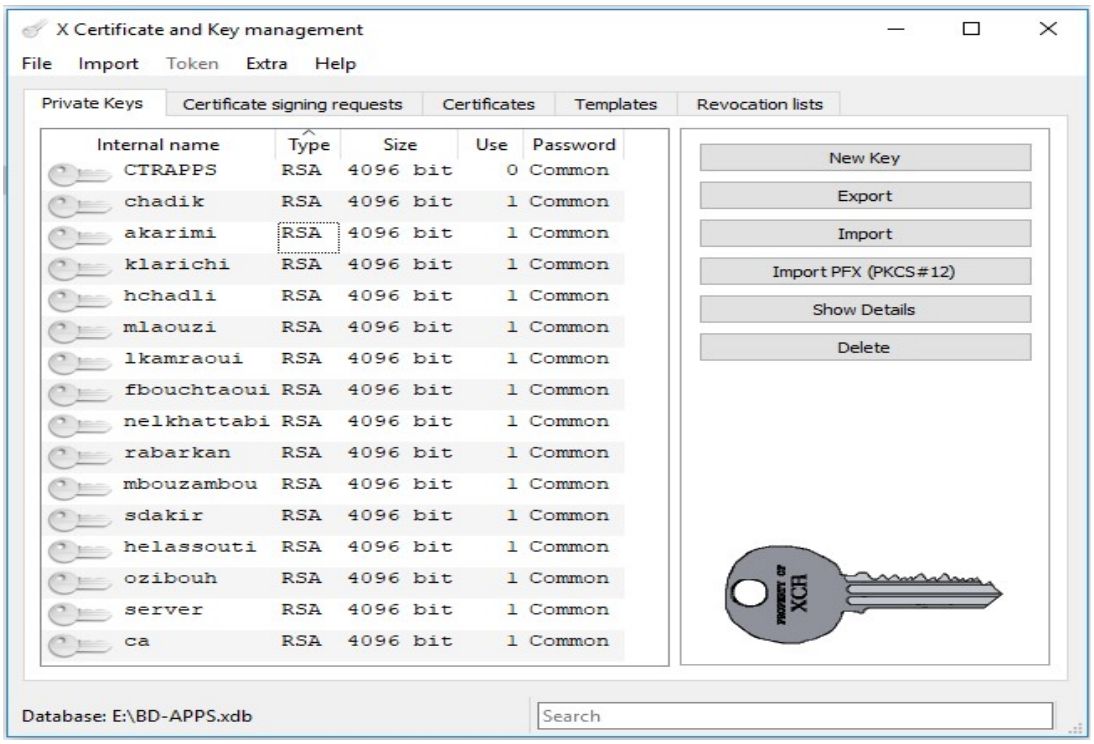

Figure 8: Private key generated with RSA algorithm

The implementation of SSL security system was provided by a system of extensive logging. The log files are located at the authentication server (CA server SSL) that containing all SSL access information.

The security of CA's private key is crucial for public key infrastructure. Knowledge of a CA private key would allow attackers to impersonate the rightful owner during all communications and transactions. They can transparently supplant any certificates signed by that private key and forging their own trusted certificates, thus appearing to be from a trustworthy source because it is signed using a legitimate (stolen) certificate. Therefore, CA's private key must be well protected and in the possession of authorized users only. To realize this, we stored the CA's private key on a secured sever in the intranet which has restricted access.

4. DISCUSSION

Many techniques are suggested for data protection in cloud computing, but most of these solutions cannot ensure confidentiality, integrity, authentication and non-repudiation as a one suite. Hence, there is a need of an appropriate security solution that should be capable to provide all basic security services not only to cloud users but to data also, either in transit or at rest.

Our proposed approach combines Public Key Infrastructure which is a very appealing and exciting technology that offers many security services for establishing trusted electronic communications with VPN IPSec technology which provides an enhanced level of security that creates VPN tunnels and encrypts the traffic sent to and from the user, providing defense-in-depth against network-based attacks. The growing need for secure cloud data storage services and the attractive properties of the both technologies lead us to combine them, thus, defining an alternative means of achieving security of the data stored in the cloud. Our proposed architecture has several advantages. It ensures the safety and privacy of data during its entire life-cycle; the data is encrypted the whole process and is not available or disclosed to unauthorized person. It can also ensure the assurance that the users have the identity they claim to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

have in the cloud. In addition, it ensures the assurance of non-alteration of the data by using the hash function; the data transmitted from source is exactly the same that has been received at destination. Finally, it ensures the non-repudiation, so neither sender or receiver of a message can later deny having processed the data.

Evaluation of implemented model performance is crucial and beneficial to both service providers and service users. The results were satisfactory and show good performance. It was observed that servers remain accessible continuously and no high computational power or memory or high bandwidth was required to implement this model. Therefore, the proposed PKI model is proven to be stable, secure and attack-proof for many conditions. This can be implemented and configured under cloud environment to secure the critical data.

One of the main weaknesses of the PKI technology is the root and private keys protection. Therefore, any organizations deploying internal PKI should have a strong key management system in place and follow best certificate practices.

5. CONCLUSION

Security of sensitive information is one of the major drawbacks and main hurdle for the adoption of data outsourcing in the cloud storage systems. Designing and implementing a secure architecture to ensure the security of the critical data stored in the cloud is an urgent need which must be given utmost importance. In this paper, we proposed Public Key Infrastructure based cryptography in cloud environment combined with VPN IPSec in order to ensure data exchange and provide a secure communication channel using SSL. Thus securing users accessing cloud services either locally, remotely or through VPN. In our research, we have implemented this model on a public institution in morocco at the national level. Results were successful in a way that different users from different branches of the public institution were authenticated. This implementation makes it possible to achieve secure electronic data transfer and access to deployed applications in the private cloud of the institution. Moreover, our proposed approach can be adopted and implemented by any public, private sector or any organization at national level. Finally, our work on the cloud security is continuing to address and resolve several other questions and will be presented in future papers in order to provide a trustworthy cloud computing environment.

REFERENCE:

[1] O. Zibouh, A. Dalli, and H. Drissi, “Cloud computing security through parallelizing fully homomorphic encryption applied to multi-cloud approach”, Journal of Theoretical and Applied Information Technology, Vol. 87, No. 2, 2016, pp. 300-307.

[2] Verizon, “2018 Data Breach Investigations report”, 2018.

[3] O. Zibouh, A. Dalli, and H. Drissi, “Encryption as a Service Based on Parallelizing Fully Homomorphic Encryption Implementation on Openstack Cloud Computing”, *International Journal of Applied Engineering Research*, Vol. 12, No. 22, 2017, pp. 12982- 12988.

[4] R. Verma and S. Agrawal, “Data Security For Any Organisation By Using Public Key Infrastructure Components And MD5, RSA, Algorithms”, *International Journal of Research in Engineering and Technology*, Vol. 02, No. 05, May 2013, pp. 819-825,

[5] J. Yu and M. Ryan, “Evaluating Web PKIs”, *Software Architecture for Big Data and the Cloud*, Elsevier, 2017, pp. 105-126.

[6] V. Lozupone, “Analyze encryption and public key infrastructure (PKI)”, *International Journal of Information Management*, Vol. 38, No.1, February, 2018, pp. 42-44

[7] S. A. Oli and L. Arockiam, “Confidentiality Technique to Encrypt and Obfuscate Non-Numerical and Numerical Data to Enhance Security in Public Cloud Storage”, *World Congress on Computing and Communication Technologies (WCCCT)*, Tiruchirappalli, Tamil Nadu, India, 2017, pp. 176-180.

[8] P. Sirohi and A. Agarwal, “Cloud computing data storage security framework relating to data integrity, privacy and trust”,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, September 4-5, 2015, pp. 115-118.

[9] C. Mathews, "Cloud Data Integrity using Password Based Digital Signatures", *International Journal of Computer Science and Information Technologies (IJCSIT),* Vol. 7, 2016, pp. 101-103.

[10] I. Memon, M. R. Mohammed, R. Akhtar, H. Memon, M. H. Memon, and R. A. Shaikh, "Design and Implementation to Authentication over a GSM System Using Certificate-Less Public Key Cryptography (CL-PKC)", *Wireless Personal Communications*, Vol. 79, No.1, November, 2014, pp. 661-686.

[11] M. Krotsiani and G. Spanoudakis, "Continuous Certification of Non-repudiation in Cloud Storage Services", *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Beijing, China, 2014, pp. 921-928.

[12] K. Lei and Z. Wang, "A CA-based scheme of user authentication over Content-Centric Networking", *The 7th International Conference on Computer Science & Education (ICCSE 2012)*, Melbourne, Australia, July 14-17, 2012, pp. 1053–1058.

[13] A. R. Metke and R. L. Ekl, "Security Technology for Smart Grid Networks", *IEEE Transactions on Smart Grid*, Vol. 1, No. 1, June 2010, pp. 99-107.

[14] F. U. Arifeen, R. A. Siddiqui, S. Ashraf, and S. Waheed, "Inter-Cloud Authentication through X. 509 for defense organization", *Proceedings of 2015 12th International Bhurban Conference on Applied Sciences & Technology (IBCAST),* Islamabad, Pakistan, January 13-17, 2015, pp. 299–306.

[15] A. AlHajri, Z. Al-Khanjari, N. Kraiem, and Y. Al Jamoussi, "Enhanced e-Government Integration Framework for Higher Interoperability in e-Government Initiatives", *2017 IEEE International Conference on Intelligent Computing, Instrumentation and Control Technologies*, Kannur, India, 2017, pp. 1831–1846.

[16] E. Rajabi, M. Kahani, and M.-A. Sicilia, "Trustworthiness of Linked Data Using PKI", *World Wide Web Conference (www2012)*, Lyon, France, April 16-20, 2012.

[17] Boyang Wang, Baochun Li, and Hui Li, "Oruta: privacy-preserving public auditing for shared data in the cloud", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 1, January-March, 2014, pp. 43-56.

[18] Monisha.M.S and Chidambaram.S, "Enhanced Data Security using RSA Digital Signature with Robust Reversible Watermarking Algorithm in Cloud Environment", *International Journal Of Electronics & Communication Technology*, Vol. 8, No. 1, January-March, 2017, pp. 20-24.

[19] L. Caviglione, M. Gaggero, E. Cambiaso, and M. Aiello, "Measuring the Energy Consumption of Cyber Security", *IEEE Communications Magazine*, Vol. 55, No. 7, 2017, pp. 58-63.

[20] G. Goyal, K. Singh, and K. R. Ramkumar, "A detailed analysis of data consistency concepts in data exchange formats (JSON & XML)", *International Conference on Computing, Communication and Automation (ICCCA2017)*, Greater Noida, India, May 5-6, 2017, pp. 72-77.

[21] V. M. Vaze, "Digital Signature on-line, One Time Private Key [OTPK]", *International Journal of Scientific & Engineering Research*, Vol. 3, No. 3, March, 2012, pp. 1-5.

[22] M. Schukat and P. Cortijo, "Public key infrastructures and digital certificates for the Internet of things", *2015 26th Irish Signals and Systems Conference (ISSC)*, Carlow, Ireland, June 24-25, 2015.

[23] V.Anand and J. S. Jafar Saniie, "Superdistribution- Testability, Security and Management of Digital Applications", *2012 IEEE International Conference on Electro/Information Technology*, May 6-8, 2012.

[24] V. Hawanna, V. Y. Kulkarni, and R. A. Rane, "Risk assessment of X.509 certificate by evaluating Certification Practice Statements", *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, Pune, India, December 19-21, 2016, pp. 501-506.

[25] S.-Y. Tan, W.-C. Yau, and B.-H. Lim, "An implementation of enhanced public key infrastructure", *Springer Science+Business Media New York*, May, 2014.