Vol. 5, No. 6 June 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Advanced Security Models for Cloud Infrastructures

[1] Logica Banica, [2] Emil Burtescu, [3] Cristian Stefan
[1,2,3] University of Pitesti, Romania

[1] olga.banica@upit.ro, [2] emil.burtescu@upit.ro, [3] cristi.stefan@upit.ro

ABSTRACT

Cloud Computing is the next-generation Internet paradigm that is offered to the business environment, educational domain and, generally, to individual users. While educational institutions and individuals quickly embraced this new technology, companies were reluctant, most of their doubts being related to the security problems. With that in mind, companies prefer Private Cloud model due to their tight security policies for data and applications. Also, a preference to address the security problems on the client-side always existed and will continue to do so in order to keep control on the confidentiality of company data. In this paper we focused on the analysis of several security methods applied in Cloud Computing environments and we proposed two security models that can overcome the safety issues.

Keywords: *Cloud Computing, Security, Data privacy, Encryption, Confidentiality.*

1. INTRODUCTION

This paper is a continuation of our research related to a cutting-edge IT domain: the next-generation Internet architectures.

Cloud Computing implementations, and especially Public Clouds, have been quickly adopted by individual and academic users, and they are growing fast in the business environment because of the well-balanced cost-to-performance ratio compared to privately-owned hardware and software platforms.

The most important drawback, as seen by the companies looking forward to migrate to the Cloud, is confidential data security and application protection.
Many IT experts focused on finding solutions to these concerns, and many of the proposed models are already deployed in Private and Public Clouds at the moment. Most efficient solutions combine advanced encryption with multi-layer authentication, but the race is still open. Maybe the future will bring a de-facto model that will become an industry standard.

In this paper we will discuss some security models that we consider most appropriate for Cloud systems and we will introduce a strategy that pairs client encryption mechanisms with the well-known OAuth standard (Open Authentication).

2. LITERATURE REVIEW

2.1 The Cloud Computing Concept

Before making an analysis of the high-level security methods applied within Cloud systems, a brief description of the Cloud Computing concept is given.

According to the National Institute of Standards and Technology (NIST), the final version of the definition for Cloud Computing is the following: „a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

This definition includes the basic elements of the concept [1]:

- The features of cloud computing: resource pooling, broad network access, on-demand self-service;
- The cloud service models (software, platform and infrastructure),
- The deployment models (private, community, public and hybrid) that provide direction to deliver cloud services.

The main features of cloud computing solutions can be summarized as follows [2]:

- Use of Internet technologies that involve the capacity of on-demand resource allocation based on current client requirements, and ubiquitous remote access
- Maintenance and security assured by providers, or a combination with the security methods implemented by the client; this offers more efficiency, extended know-how and zero-effort scalability of the hardware and software resources.
- Elastic storage volumes and almost infinite capacity
- Highly-redundant, certified security and minimal-downtime features that empower the client business at a fraction of private infrastructure costs

This way, clients can deploy their applications when they need it, where they need it, as the cloud is accessible from anywhere there's an Internet connection, on any platform.

NIST defines three fundamental models for Cloud computing services: Infrastructure as a Service

(IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [3][4]. In addition to the three models, on the IT market a fourth model of cloud services: Business Process as a Service (BPaaS) has emerged.

We summarized the services provided by each layer as they are described on NIST website:

- Infrastructure as a Service (IaaS) is the service model that allows the customers to use computing resources such as servers, storage devices and network infrastructure (addresses, load balancers and firewalls), often delivered as virtual machines hosted by the service provider and managed remotely;
- Platform as a Service (PaaS) is the model that provides to the users the capability to build, test and deploy their applications on the cloud infrastructure. This layer offers a collection of programming languages, databases, specialized tools and middleware that are able to host full-size applications deployed by the client. PaaS is completely managed by the provider, but end-users can customize their environment settings and deploy everything they need
- Software as a Service (SaaS) is the most popular model, and requires that cloud providers install and operate the complete application stack on their platform and users access these applications remotely through specific client software. In this manner, the customers do not manage the cloud infrastructure on which their application is running, and are not responsible for maintenance and support.
- Business Process as a Service (BPaaS) is an emerging model offering additional business functions, such as payment processing, human resources management. The model is available over the Internet, or the company's Intranet network [5][6].

Figure 1 shows the latest layered architecture of the Cloud Computing in business environment, education and social domain.

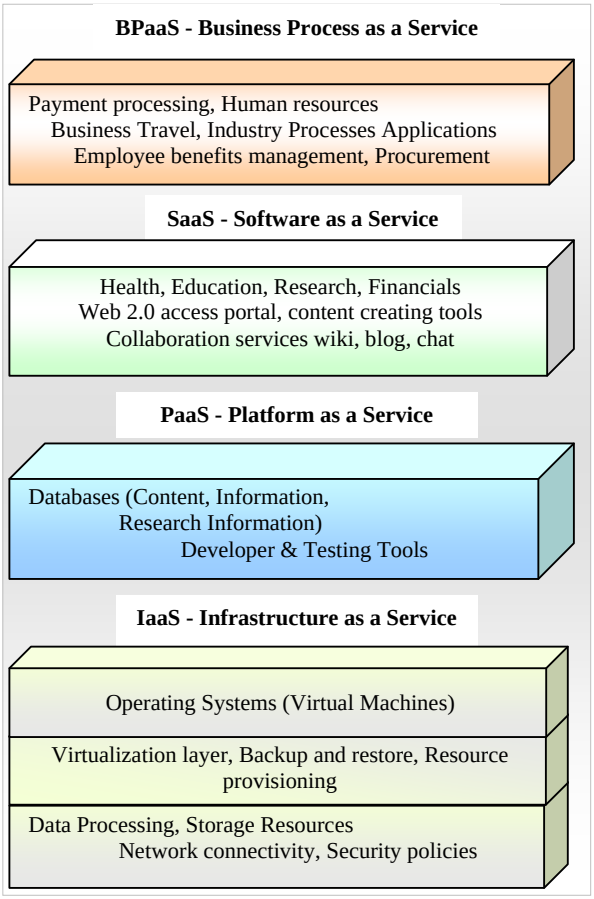

Fig 1: The layered architecture of Cloud Computing
Source: an updated version of Fig. 2 from [4]

Other cloud service models available at the moment are Desktop as a Service (DaaS), Storage as a Service (StaaS) and Security as a Service.

Desktop as a Service (DaaS) is an integrated approach for the distributed computing, in which a complete VDI (virtual desktop infrastructure) is delivered to the client and completely managed by the service provider [7]. This way, all maintenance tasks are automatically executed by the cloud platform, thus relieving the client from tedious backup, application deployment and security tasks that should be fulfilled on a regular basis. It is supported by the most important players on the market, like Citrix, Cisco, VMware and Amazon.

Storage as a Service (StaaS) is more like an auxiliary component of an Internet-based business, which takes backup and data archiving from the client facility and moves it to a high-performance, always-available and secure infrastructure owned by the cloud hosting company. This way, if something happens to the servers at the client side, or the business is forced to relocate, data is accessible right away from anywhere in the world [8].

Security as a Service (SECaaS) involves outsourcing the very complex mission of securing the most precious assets of a web-based company: data and applications. By subscribing to this kind of consultancy, the client can focus on its core business, and forget about multi-product malware scanning with the most recent signature database, continuous update deployment, behavioral analysis of email traffic to remove spam, phishing and confidential data, user provisioning (account management), vulnerability detection and intrusion prevention [9].

This paper brings into discussion various issues that affect the popular SaaS distributed computing model.

NIST also defines the key implementation models for Clouds [3]:

- Public Cloud – delivers an important set of application and infrastructure services to the general public or large groups of users; the infrastructure is owned by a powerful software company, providing cloud services for free or based on a flexible price per use;
- Private Cloud – refers to an infrastructure offered over an Intranet, so all resources are owned and managed by a private organization, and the access is limited according to its internal policies;
- Community Cloud – provides a model for an infrastructure that is shared by several organizations and supports a specific community that has similar approaches about policy, objectives, and security requirements [6];
- Hybrid Cloud – approaches the model as a joint solution of public and private clouds that are bound together by standardized rules and are managed by the cloud provider.

Despite the accessibility and the various types of services offered by the Public Cloud implementations, many companies prefer to host the applications on their Private Clouds, in order to keep control of the applications and to protect and assure the confidentiality of data warehouses, transactional databases, data archives etc.

2.2 The security on Cloud Computing

Many organizations and institutions migrated to Cloud Computing in order to enhance their business competitively with same-level or lower costs, and broaden end users access by making the services and resources available through their browsers.
But adoption reluctance is related to the performance of security methods, so many still expect a model that will give them the necessary confidence in storing and accessing their private data by powerful, secured Public Clouds.

Also, there is an issue concerning the network use: the communications via the public Internet are another source of insecurity, though this is the foundation of Cloud accessibility and portability.

However, more and more enterprises are turning to Cloud Computing environments, because the advantages are becoming more and more attractive. The company management must decide the service level requirements, the need for resources (which can be computing power, memory, bandwidth or business applications licenses).

The most frequently-chosen deployment model is the Private Cloud, due to the security and ensured confidentiality of the available services provided to the employees and customers.

According to Singla and Singh [10], there are two main goals pursued by the secure Cloud implementations:

a. Privacy and Confidentiality – the Cloud service provider must assure that customer data is accessible only to authorized users and that all hosted information will be kept confidential in all circumstances;
b. Security and Data Integrity – the Cloud service provider must assure the protection of data by encryption and decryption techniques and implement a mechanism to monitor integrity of the data at the cloud [11].

In the 2012 report of Computerworld - “Cloud Computing” studies [12], some of the data security challenges in the cloud were underlined:

- The need to protect confidential business data on cloud models with multiple enterprises and organizations sharing the same infrastructure; a new type of insider who may have control and visibility on other customer’s data;
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive;
- Lack of standards about how Cloud service providers securely recycle disk drives and erase existing data;
- The enterprise IT security and risk management departments lose the control over the data security and operational intelligence activities.

We focused on the first problem, major in our opinion: the lack of an edge that can clearly separate enterprise data and applications in a shared Cloud environment.

There are many possible entry points for an intruder in a Cloud environment, as follows [13]:

a. a customer uses an insecure mobile phone to access the data;

b. a contractor of the network uses a web application that has an embedded vulnerability, a backdoor or one that is not protected;
c. a database administrator of the Cloud provider shares a password with another network customer.

Obviously it becomes more and more difficult to protect a Private Cloud environment having an increased number of users: employees, customers, suppliers and business partners who request access to corporate data and applications with mobile devices or by Internet connections.

As an example, the IBM Cloud security policy includes new ways to ensure protection from unauthorized access to the Cloud [13]:

a. Establishment of security levels for the users of each organization (privileged and common users); Database administrators and supervisors are privileged users, having more control rights than common users.
b. Changing the level of access to the Cloud data depending on the source access point of the user: full rights inside company the network and limited access for mobile access.
c. Identification highly sensitive or valuable data and provide extra protection by encryption and monitoring for them;
d. Adding intelligent network protection to enforce the control of the content and accessible applications.

The important role of Cloud Computing [14] cannot be denied, but its drawbacks may not be overlooked for several reasons:

- For security reasons, company managers might not agree to run critical applications on the Cloud and send sensitive data to the Cloud for processing and storage;
- For accessibility reasons, clients want permanent access to the information even when the Internet and Cloud are down or the network communication is slower.

In comparison with Grid models, Cloud implementations are less secure and the risks are the main concern for the providers.

We underline several requirements that a Cloud customer should be asking to the provider before adopting this computing paradigm [15]:

- Granting privileged user access: sensitive data processed outside the enterprise needs the assurance that they are accessible only to designated users;
- Verifying the security certifications: the customer should verify that the Cloud provider has audits and security certifications;
- Separating Data: the client must ensure that its data is completely separated logically from other customer's data;
- Automatic backup and recovery mechanism: the Cloud provider must implement an automated replication and recovery mechanism to restore data in case of unwanted events;

A secure channel between endpoints is created by means of encrypted communication protocols, such as HTTPS, VPN, TLS or SSH. Thus, MitM attacks (eavesdropping, spoofing or session hijacking) become impossible.

3. METHODOLOGY

In many countries PKI (Public Key Infrastructure) certificates are released by a trusted organization, a Certification Authority (CA) that verifies the identities and validates the servers involved in communications. Another aspect is the content of a PKI certificate, which involves a pair of public and private keys.

We consider that the private key is a secure tool to protect the enterprise data, because it is never transmitted outside.

For SMBs (Small and Medium Businesses), which do not have the required financial and hardware resources to implement a trusted PKI in their own datacenter, the suggestion would be to use the publicly available OAuth standard.

3.1 Auth Standard

Due to some business requirements, users need to access several resources in the Cloud and it is difficult to manage different passwords and authentication methods for each client.

Cloud providers can solve these problems by implementing a secure SSO (Single-Sign-On) solution, so each user is granted access to multiple applications after supplying its credentials only once. After validation, the client receives a ticket (cookie) that enables the access of all the resources.

The next level of authentication and authorization is based on OAuth standard and implies three entities: the user, the client application and the service provider/authorization server. OAuth standard enables the user to grant client application/service access to its resources without sharing its username/password with the client application. This standard is preferred for Cloud services but also for social media and mobile applications.

Even though SSO and OAuth solutions are important improvements in Cloud security, PKI (Public Key Infrastructure) is the strongest form of authentication.

3.2 Confidentiality in Clouds by Using Cryptography

As a security method, encryption doesn't stop attacks, but it minimizes the possibility that the intruder reads the owner data. The message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable cipher-text [16][17]. The opposite process of encryption (restoring the original data from encrypted data) is called decryption. An authorized party is able to decode the cipher-text using a decryption algorithm, which usually requires a secret decryption key.

There are many encryption/decryption methods that use powerful algorithms, classified in three big categories: Symmetric-key algorithms, Asymmetric-key algorithms and Hashing [18].
Even if the asymmetric-key algorithms performance is better in comparison with symmetric-key algorithms for Cloud storage, there is the drawback of slower speed.

In the following part, we will discuss some of the most common encryption methods:

- **Symmetric-key algorithms** use the same key for both encryption and decryption, they have the advantage of not consuming too much computing power and they work with high speed in encryption [19]. In Cloud computing DES (Data Encryption Standard), Triple-DES, and AES (Advanced Encryption Standard) algorithms are more frequently used.

DES is the most widely used algorithm and it uses a 64-bit plaintext and same 56 bit cipher key for both encryption and decryption. The encryption process is made of two permutations (P-boxes), and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm [19].

A way of increasing the security is the Triple DES algorithm, which comprises three DES keys, each of 56 bits, applied to one block of 64 bits of data.

AES (Advanced Encryption Standard) encrypts 128-bit blocks with the key size of 128, 192, or 256 bits. AES operates on a 4×4 column-major order matrix of bytes, known as the state [19].

Blowfish is a reversible method of protection, based on a single password (secret) that is used both for encryption and decryption. It uses a block size of 64 bits, a variable–length key, from 32 bits to 448 bits and it is appropriate for applications where the key is not changed frequently. It has proven to be much quicker on 32-bit machines than the other methods, thanks to their generous cache [20].

MD5 is also a well-known cryptographic method based on a hash function, which processes a variable length blocks (multiple of 512-bits) into a fixed-length output of 128 bits. To encrypt data, sender uses the public key of the receiver and the receiver uses its private key to decrypt data [21].

- **Asymmetric-key algorithms** use different keys for encryption and decryption: a private key and a public key. Although different, the two parts of this key pair are mathematically linked. The public key is used by the sender for encryption and the private key is used for decryption of data by the receiver [18].

The main advantage of this solution is represented by the mathematical impossibility of deducing the private key from the public key. Everybody can have the public key without any concerns about confidentiality, given that the private key is kept secret and used only by authorized entities.

In Cloud Computing RSA, IKE, Diffie-Hellman Key Exchange asymmetric-key algorithms are used.

Homomorphic Encryption implies that the Cloud user encrypts its data before sending it to the CSP (Cloud Service Provider) and each time access is required, it will decrypt the data locally. Homomorphic Encryption systems are needed to perform operations on encrypted data without decryption (without knowing the private key), only the consumer having the secret key.

RSA algorithm realizes the properties of the multiplicative Homomorphic encryption [20]. It uses modular exponential for encryption and decryption with a public key for encrypting messages and a private key to decrypt them.

4. PROPOSED SOLUTIONS

Studies made in the security and encryption fields for Cloud infrastructures have led us to proposing two solutions for ensuring business data confidentiality at the BPaaS level:

Also, for both variants we consider that is necessary to separate the enterprise data in two parts: sensitive internal data (data shell) and external data (suppliers, clients, product catalogues etc).

By separating data flows in the company datacenter, a symmetric-key algorithm is applied, which offers the Cloud customer a high level of trust regarding the security and confidentiality of its critical data. In the same environment, many customers can keep their data safely, as each has a personal encryption key that will never be shared.

Such a division is as important as choosing the correct application point for the encryption and authorization algorithms, and gives the Cloud users full

control of their own data, while the CSP ensures data protection globally for the centralized infrastructure, without knowing the contents of client data.

Thus, the first proposed solution (Model 1) is for Public Cloud security and combines OAuth standard authentication methods with encryption algorithms (Figure 2).

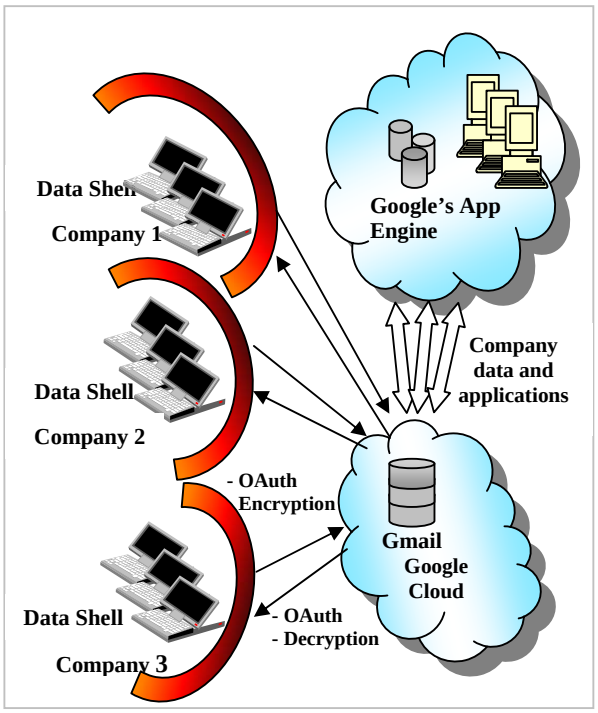

Fig 2: Model 1- Security on Public Clouds

The success of OAuth standard in the social media domain has led to its adoption for enterprise authentication management in Clouds.

A sample use-case may be Google's ecosystem, as it offers business e-mail, calendar, Office apps and storage, but also a powerful platform for running web applications, called Google App Engine. A single account (OAuth) is enough for accessing the infrastructure, and the company can easily manage the user database and access privileges.

The steps to control user's access to the company applications are as follows [22]:

- The user provides its credentials and requests access to the company applications;
- The username and password are redirected to Google Cloud for authentication;
- After validation, user is redirected back to the system with OAuth credentials and now he has the ticket to be granted access to company applications.

Data transmission is made after applying a symmetric-key encryption algorithm, such as DES, Triple-DES or AES.

Solutions to cloud security issues are various, from cryptography and public key infrastructure (PKI) to use of multiple cloud providers.

The second proposed solution (Model 2) involves certificate-based authentication, followed by public key cryptography applied to the confidential business data before storing it in the Cloud.

Within a PKI, a certificate authority must create and sign a company's key. Some of the clients found PKIs difficult to use, so the security providers have another variant: public key technologies such as Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), which often required no authentication of the user, but were there simply to authenticate the server and secure transactions.

Also, we consider that using PKI in the Cloud in conjunction with the secure transport mechanism, TLS, is a better solution because it offers a cryptographically strong method of authentication in an unsafe communication environment.

After authentication, private data encryption will ensure the privacy of the data sent from the client devices to the Clouds and back.

The client digitally signs data and sends both the certificate and the signed data across the network. The server uses techniques of public-key cryptography to validate the signature and confirm the validity of the certificate (Figure 3).

Windows Azure platform is an example of implementing cloud security using Public Key Infrastructure.

Certainly, this is a more secure method than password-based authentication because it is based on Public key cryptography that can verify that a Private Key used to sign some data corresponds to the Public Key in a certificate. The client has the responsibility to keep the private-key password secret.

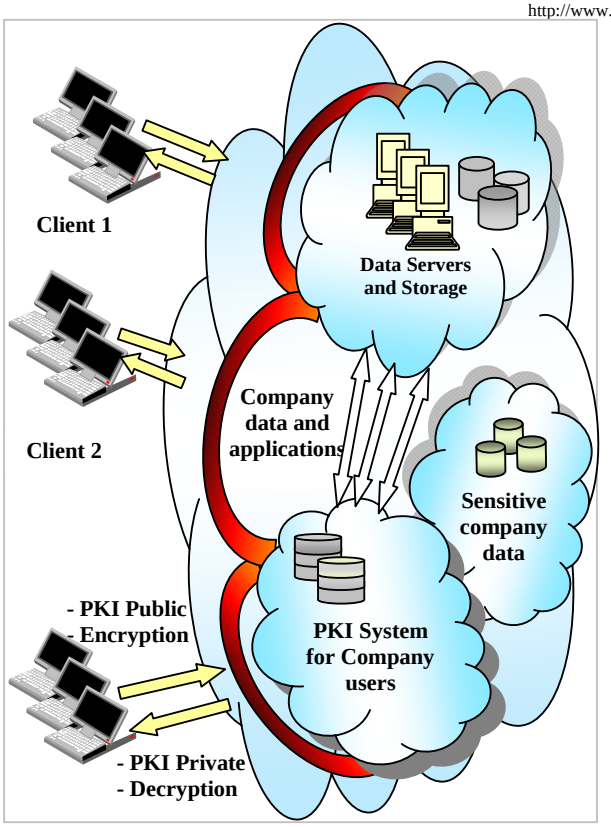

Fig 3: Model 2- Security on Private Clouds

The SSO model is replacing the password exchange that will normally occur when having different login points. This way, a user will enter its password once and unlock the private key database. Then, a signed certificate will be passed on to the necessary services for authentication.

The main phases for authentication, authorization and protect the confidentiality in this manner are as follows:

- The Cloud provider/CA maintains a database of the private keys that correspond to the public keys published in any certificates issued for their clients.
- The Client uses that private key to digitally sign its data. The digital signature can be created only with that private key and can be validated with the corresponding public key against the signed data.
- The Client sends both the user's certificate and data that has been digitally signed across the network.
- The Cloud server uses the certificate and the evidence to authenticate the Client's identity. The server may perform other authentication tasks, such as checking that the certificate presented by the client is stored in the user's entry in an LDAP directory. Also, it may evaluate whether the identified user is permitted to access the requested resource. If all the evaluation results are positive, the Cloud server allows the Client the access the requested resources.

Transmitted data is encrypted by using a symmetric-key algorithm, such as Homomorphic Encryption or RSA.
For business environment, Symantec Company offers a performant managed PKI solution, but it may not be cost effective for small to mid-size businesses.

An already-in-use, pay-as-you-grow solution comes from Tresorit AG, which offers 5GB of AES-256 encrypted storage in their ISO/SSAE-certified Cloud for free, and flexible pricing for business use. Their main advantage is that no client data leaves the end device unencrypted, protecting it by TLS even from client's ISP and also from any of the Cloud Provider's employees.

5. CONCLUSIONS

From the studies performed on different Cloud infrastructure security methods, it is revealed that there are many protection models, each with its own advantages and drawbacks, but there is no perfect solution for all kinds of use-cases.

If the customer is academia, ordinary users or small and medium enterprises, the first model proposed in the paper can satisfy their security requirements in low-cost and performance conditions. For bigger, privately-own companies the security is more important even than the high performance and we recommend the second model proposed.

We are aiming to continue the Cloud environment security investigations by testing and comparing performance of the presented encryption schemes in Public Cloud systems.

REFERENCES

[1] Mell, P., Grance, T., (2011), National Institute of Standards and Technology - Definition of Cloud Computing, available on http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html

[2] Cacciari, C., D'Andria, F., Gonzalo, M., Hagemeier, B. et al., (2010), ElasticLM: A novel approach for software licensing in distributed computing infrastructures, Procedures IEEE 2nd International Conference on Cloud Computing Technology and Science, pp. 67–74.

[3] Final Version of NIST Cloud Computing Definition, NIST Special Publication 800-145, published on October 2011, available on http://www.nist.gov/itl/csd/cloud-102511.cfm

[4] Banica, L., Stefan, C., (2013), From Grid Computing to Cloud Infrastructures, International

Journal of Computers & Technology, Vol 12, No.1, pp. 3187-3194

[5] Sreekanth I., (2010), Cloud Deployment and Delivery Models, available on https://www.ibm.com/ developerworks/community/blogs/sreek/entry/cloud_4?lang=en

[6] Harding, C. et al., (2011), Cloud Computing for Business, Open Group, http://www.opengroup.org/ sites/default/files/contentimages/Press/Excerpts/first_30_pages.pdf, pp.28-31.

[7] Technical White paper VMWare &Symantec, Desktop as a Service with VMware and Symantec (2011), available on: https://www.vmware.com/files/pdf/b-desktop_as_a_service_WP_en-us_08-11.pdf

[8] Kulkarni, G., Sutar, R., Gambhir, J., (2012), Cloud Computing-Storage as Service, International Journal of Engineering Research and Applications, Vol. 2, Issue 1, pp.945-950

[9] Rashmi, R., Sahoo, G., Mehfuz, S., (2013), Securing Software as a Service Model of Cloud Computing: Issues and Solutions, International Journal on Cloud Computing: Services and Architecture, Vol.3, No.4, DOI : 10.5121/ijccsa.2013.3401

[10] Singla, S., Singh, J., (2013), Cloud Data security using Authentication and Encryption Technique, International Journal of Advanced Research in Computer Engineering & Technology, Vol. 2, Issue 7, pp. 2232-2235.

[11] Singla, S. Singh, J., (2013), Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm, Global Journal of Computer Science and Technology (GJCST), Vol. 13, Issue 5.

[12] Tumulak, D., (2012). Data Security in the Cloud, Computerworld "Cloud Computing" study, http://www.vormetric.com/sites/default/files/wp-data-security-in-the-cloud.pdf

[13] Marx, G., (2013). Can cloud computing be secure? Six ways to reduce risk and protect data, http://www.theguardian.com/media-network/media-network-blog/2013/sep/05/cloud-computing-security-protect-data

[14] Foster, I., Zhao, Y., Raicu, I., Lu, S., (2008). Cloud Computing and Grid Computing 360-Degree Compared, Grid Computing Environments Workshop, pp. 1 – 10.

[15] Brodkin, K., (2008), Gartner: Seven cloud-computing security risks, http://www.networkworld.com/ news/2008/070208-cloud.html.

[16] Krutz, L., R. and Vines, R., D., (2010), Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, Inc. Indianapolis, Indiana 2010.

[17] Goldreich, O., (2004), Foundations of Cryptography: Volume 2, Basic Applications. Vol. 2, Cambridge University Press, 2004.

[18] Nigoti, R., Jhuria, M., Singh, S., (2013), A Survey of Cryptographic Algorithms for Cloud Computing, , International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), volume 4, Issue 2, pp.141-146, available on http://www.iasir.net

[19] Jeeva, A., L., Palanisamy, V., and Kanagaram, K., (2012), Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms, International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp. 3033-3037.

[20] Devi, G., Kumar, P., M., (2012), Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm , International Journal Of Computer Trends And Technology, Volume 3, Issue 4, ISSN: 2231-2803, pp. 592-596.

[21] Gurpreet, K., Manish, M., (2013), Analyzing Data Security for Cloud Computing using Cryptographic Algorithms, International Journal of Engineering Research and Applications, Vol. 3, Issue 5, pp.782-786.

[22] Pisarkiewicz, C., (2014), How to Use OAuth for Enterprise Identity Management available on http://www.forumsys.com/oauth/use-oauth-enterprise-identity-management/