ESS-Cloud

Neha Chalke[#1], Pratik Ghogale[#2], Mr. Rahul Sirsilla[#3], Archana Salaskar[*4]
[#] Student, Dept. of Information Technology.
[*]Lecturer, Dept. of Information Technology.
Shah & Anchor Kutchhi Polytechnic, Mumbai, India
nnchalke@gmail.com[1], *sunnyghogale@gmail.com*[2],
rahulsirisul97@gmail.com[3], *archana.salaskar@gmail.com*[4]

***Abstract*:**-Many people have security problems to store their data over a cloud. In this paper, we describe how we can store our data more secure over the cloud using Cryptography. We are using an encryption technique which will encrypt the data when stored on the cloud and it will again be decrypted when it is to be retrieved by the user in the original form of data. Enhanced security will ensure that the data stored in the cloud won't be accessible from the server without proper authentication. Storing data on cloud will ensure that we can access our data from anywhere and at any point of time.

Keywords:-*Cloud Computing, Private Cloud, 3DES, Encryption, Decryption, Cloud Security.*

*****

1. INTRODUCTION

Cloud computing is a technology that keep up data and its application by using internet and central remote servers [1].While many are pushing back on cloud computing due to security concerns, cloud computing is, in fact, as safe as or better than most on-premises systems. You must design your system with security, as well as data and application requirements in mind, then support those requirements with the right technology. You can do that in both public or private clouds, as well as traditional systems. Companies that don't understand the risk just shouldn't use cloud computing. The potential for a security breach or a compliance violation can be high. While security emerges as a major concern among the barriers to the adoption of cloud computing. Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind cloud security architecture, they can usually be found in Deterrent, Preventive, Detective, Corrective controls.

In this paper we will either integrate the customer's identity management system into their own infrastructure, using Single Sign-on technology, or a biometric-based identification system, or provide an identity management solution of their own CloudID.

Single Sign-on technology :- (**SSO**) is a property of access control of multiple related, but independent software systems. With this property a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on servers [19]. A simple version of single sign-on can be achieved over IP networks using cookies but only if the sites share a common DNS parent domain [20].

Biometric-based identification system: - Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control [21].Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals [22]. Biometric identifiers are often categorized as physiological versus behavioral characteristics [23]. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice [24].

Making use of Triple DES encryption technique, performed in encrypted domain to make sure that any potential attackers do not gain access to any sensitive data or even the contents of the individual queries. We are implementing a cloud which will have a login id and a password which will act as a key for the encryption technique. The key will help to encrypt the data that is going to be stored over the cloud using the Triple DES Encryption Algorithm. The data will be stored in cipher text format. The data will be retrieved in the original format after the user wants it to be retrieved. If a hacker hacks the cloud account, he gains access to the cloud but he won't be able to retrieve the data present in it as it is in the encrypted format.

2. BACKGROUND

The term Cloud Computing is an emerging modern technology which has been evolved and developed in last few years, and also considered as the next big refined way to store data. Since it is new, so it requires new security issues and face new Challenges as well. Providers ensure that all critical data are masked or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

The significance of cloud computing and what it brings may go unnoticed. Security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution [15], Cloud computing and its services are something we use every day, sometimes without notice. Some popular cloud services people use often or daily are, Gmail, YouTube, or Google Docs. Cloud computing and its services bring multiple different components to the people and the internet which are very helpful in today's world. Cloud computing stores your files online, it allows you to get your apps online, also backs up your computer for less, and also get you the latest updates faster. Before cloud computing these things were harder and much more complicated to do. Before cloud computer saving or storing your files was much more complex. To save them you had to first save them on a hard-drive, or personal computer, and to take them with you, you'd have to save them to a thumb drive or CD. Now that cloud computing is introduced, you can save them online, and access them not only from your computer, but from anywhere. Before cloud computing, to back up your files you had to buy expensive hardware in order to save them. Now that cloud computing is introduced online backup services are now available because of cloud services. Before cloud computing and its services, you had to wait hours with technical people when your applications wasn't working properly. Now that cloud computing is the leading strategic technology service, that isn't an issue anymore. Now cloud apps usually are updated automatically by their provider and also maintained by them as well. As it shown, cloud computing is a very helpful source or tool in today's society.

2.1 LITERATURE SURVEY

Individuals and enterprises take advantage of the benefits for storing large amount of data or applications on a cloud. However, issues in terms of their integrity, authentication, and digital rights must be taken care of [3].

- **SaaS**

Software as a service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted [5] [6]. It is sometimes referred to as "on-demand software"[7]. SaaS is always used by users using a thin client.

- **Security issues in SaaS:**

Software as service is a model, where the software applications are hosted slightly by the service provider and available to users on request, over the internet. In SaaS, client data is available on the internet and may be visible to other users, it is the responsibility of provider toss set proper security checks for data protection.

- **PaaS**

Platform as a service (PaaS) is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage web applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app[8][9][10].

- **Security issues in PaaS**

It deals with operating system, middleware.. In PaaS, the service providers give some command to customer over some application on platform. But still there can be the problem of security like intrusion etc, which must be assured that data may not be accessible between applications.

- **IaaS**

This model provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data center space etc. are pooled and made available to handle workloads. The capability provided to the customer is to rent processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has the control over operating systems, storage, deployed applications, and possibly select networking components [16].

Infrastructure as a service is taking the physical hardware and going completely virtual (e.g. all servers, networks, storage, and system management all existing in the cloud).This is the equivalent to infrastructure and hardware in the traditional method running in the cloud. In other words, businesses pay a fee to run virtual servers, networks, storage from the cloud. This will mitigate the need for a data center, heating, cooling, and maintaining hardware at the local level [11].

- **Security issues in IaaS**

The IaaS provides basic security firewall, load balancing, etc. In IaaS there is better control over the security, and there is no security gap in virtualization manager. The main security problem in IaaS is the trustworthiness of data that is stored within the provider's hardware.

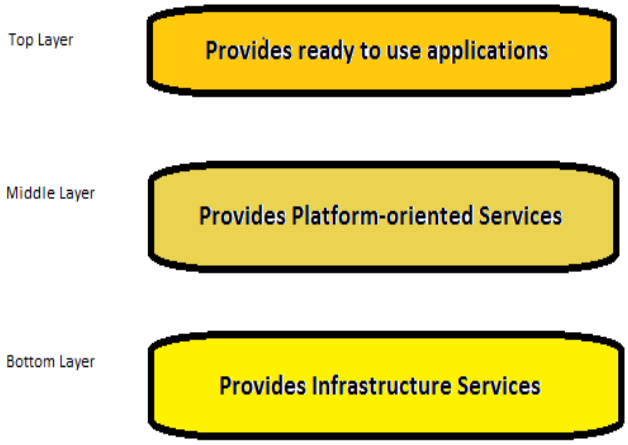

Top Layer
Provides ready to use applications
Middle Layer
Provides Platform-oriented Services
Bottom Layer
Provides Infrastructure Services

Figure 1. Types of Services provided by Cloud

2.2 Guidelines on Security and Privacy in Public Cloud Computing [2]

Guidelines on Security and Privacy in Public Cloud Computing (NIST Special Publication 800-144) provides an overview of the security and privacy challenges Facing public cloud computing and presents recommendations that organizations should consider when outsourcing data, applications and infrastructure to a public cloud environment. The document provides insights on threats, technology risks and safeguards related to public cloud environments to help organizations make informed decisions about the use of this technology.

The key guidelines include:

- Carefully plan the security and privacy aspects of cloud computing solutions
- Understand the public cloud computing environment offered by the cloud
- Ensure that a cloud computing solution—both cloud resources and cloud-based applications—satisfy organizational security and privacy requirements.
- Maintain accountability over the privacy and security of data and before implementing them and deployed in public cloud computing environments.

2.3 Types of Attackers in Cloud Computing

Many of the security threats and challenges in cloud computing will be familiar to organizations managing in house infrastructure and those involved in traditional outsourcing models. Each of the cloud computing service delivery models' threats result from the attackers that can be divided into two:

2.3.1 Internal attackers

An internal attacker has the following characteristics:

• Is employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service

• May have existing authorized access to cloud services, customer data or supporting infrastructure and applications, depending on their organizational role

• Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service.

2.3.2 External attackers

An external attacker has the following characteristics:

• Is not employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service

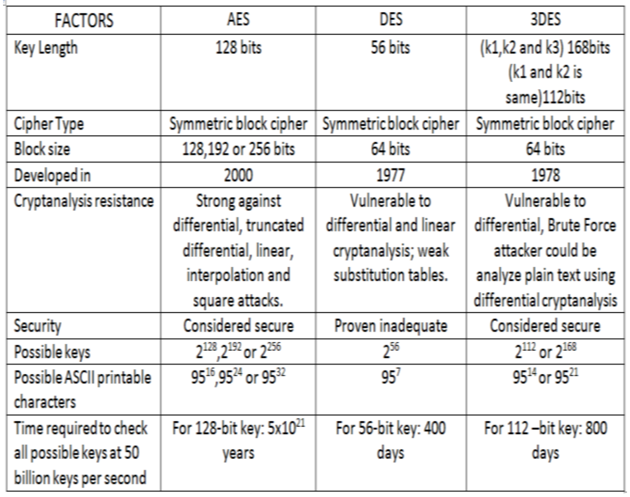
• Has no authorized access to cloud services, customer data or supporting infrastructure and applications

• Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information within the cloud service.

2.4 PROPOSED SYSTEM

We are implementing a cloud which will have a login credentials which will act as a key for the encryption technique. The key will help to encrypt the data that is going to be stored over the cloud using the Triple DES Encryption Algorithm. The data will be stored in cipher text format. The data will be retrieved in the original format after the user wants it to be retrieved. If an intruder try to intrude into the cloud account, he gains access to the cloud but he won't be able to retrieve the data present in it as it is in the encrypted format.

Table 1: Comparison between AES, DES, 3DES [4]



FACTORS	AES	DES	3DES
Key Length	128 bits	56 bits	(k1,k2 and k3) 168bits (k1 and k2 is same)112bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block size	128,192 or 256 bits	64 bits	64 bits
Developed in	2000	1977	1978
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and square attacks.	Vulnerable to differential and linear cryptanalysis; weak substitution tables.	Vulnerable to differential, Brute Force attacker could be analyze plain text using differential cryptanalysis
Security	Considered secure	Proven inadequate	Considered secure
Possible keys	2^{128},2^{192} or 2^{256}	2^{56}	2^{112} or 2^{168}
Possible ASCII printable characters	95^{16},95^{24} or 95^{32}	95^{7}	95^{14} or 95^{21}
Time required to check all possible keys at 50 billion keys per second	For 128-bit key: 5x10^{21} years	For 56-bit key: 400 days	For 112 –bit key: 800 days

In 1998 a standard ANS X9.52 and named Triple Data Encryption Algorithm (TDEA). a. Block cipher with symmetric secret key b. Block length = 64 bits c. Key length = 56, 112 or 168 bits 3DES was created because DES algorithm, invented in the early 1970s using 56-bit key. The effective security 3DES provides is only 112 bits due to meet-in-the-middle attacks. Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. In DES, data is encrypted and decrypted in 64 -bit chunks. The input key for DES is 64 bits long; the actual key used by DES is only 56 bits in length [18].

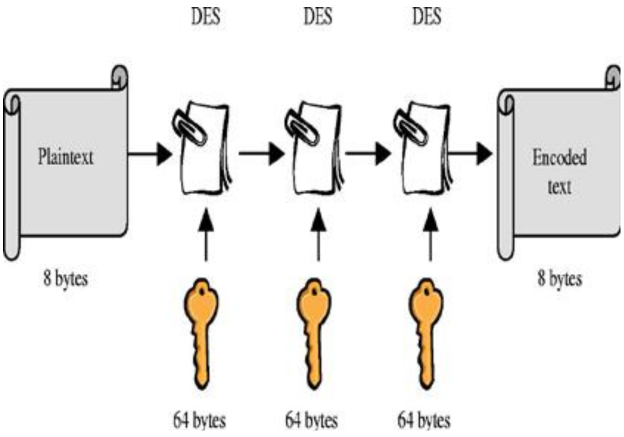


Figure 2. Triple DES Using 64 bytes [18]

The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process. Triple DES Using 64 bytes. Above Figure 2 shows Triple Data Encryption Standard (DES) which is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three keying options in data encryption standards: a. All keys being independent b. Key 1 and key 2 being independent keys c. All three keys being identical Key option 3. The triple DES key length contains 168 bits but the key security falls to 112bits [18].

2.5 Algorithm

In [18], author discussed 3DES as follows;

Run DES three times:

If K2 = K3, this is DES Backwards compatibility Known not to be just DES with K4Has 112 bits of security, not 3 56 = 168 Triple DES algorithm uses three iterations of common DES cipher. It receives a secret 168-bit key, which is divided into three 56-bit keys.

• Encryption using the first secret key

• Decryption using the second secret key

• Encryption using the third secret key

Encryption: c = E3 (D2 (E1 (m)))

Decryption: m = D1 (E2 (D3(c)))

Using decryption in the second step during encryption provides backward compatibility with common DES algorithm. In these case first and second secret keys or second and third secret keys are the same whichever key.

c = E3 (D1 (E1 (m))) = E3 (m)

c = E3 (D3 (E1 (m))) = E1 (m)

It is possible to use 3DES cipher with a secret 112-bit key. In this case first and third secret keys are the same.

c = E1 (D2 (E1 (m)))

The standards define three keying options:

- **Keying option 1**
- All three keys are independent.
- **Keying option 2**

- K_1 and K_2 are independent, and $K_3 = K_1$.
- **Keying option 3**
- All three keys are identical, i.e. $K_1 = K_2 = K_3$.

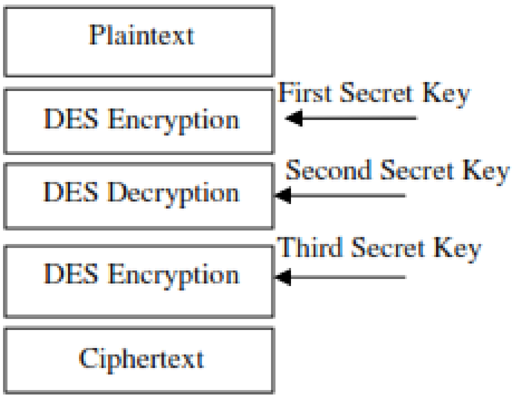


Figure 3. Block Diagrams: 3DES Encryption [18]

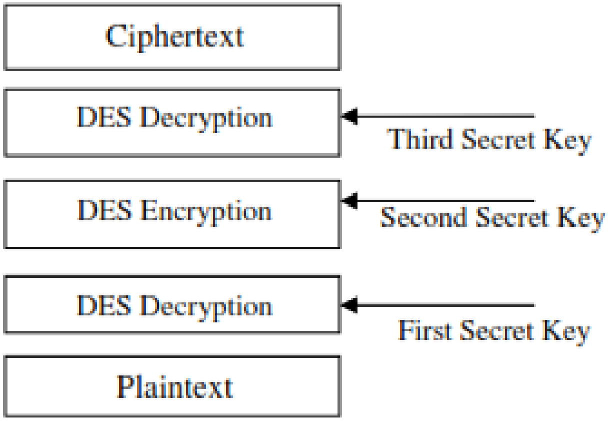


Figure 4. Block Diagrams: 3DES Decryption [18]

Keying option 1 is the strongest, with 3 × 56 = 168 independent key bits. Keying option 2 provides less security, with 2 × 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K_1 and K_2, because it protects against meet-in-the-middle attacks. Keying option 3 is equivalent to DES, with only 56 key bits. It provides backward compatibility with DES, because the first and second DES operations cancel out. It is no longer recommended by the National Institute of Standards and Technology (NIST) [12] and is not supported by ISO/IEC 18033-3.

Each DES key is nominally stored or transmitted as 8 bytes, each of odd parity [1], so a key bundle requires 24 bytes for option 1, 16 for option 2, or 8 for option 3.

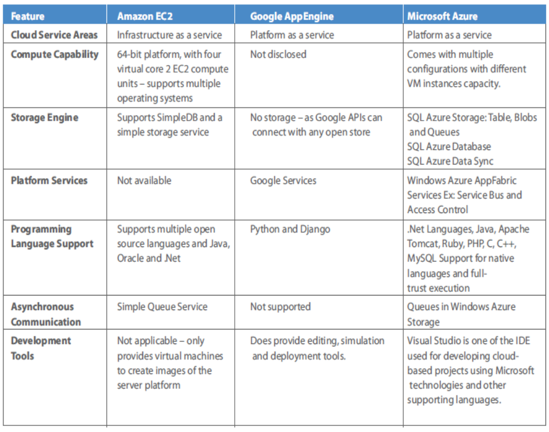
This algorithm will surely help in increasing the security for the cloud and surely decrease the risk of getting into wrong hands or intruders.

2.6 IMPLEMENTATION DETAILS

The implementation of cloud will be done by using Microsoft azure. The implementation methodology follows the simple practice of modeling the services and decides if either a completely new application needs to be developed or if the application can be composed through other mash-up services or channels. Windows Azure Compute Instances can support native code execution and applications running on the .NET framework, PHP, Java, Apache TOMCAT, MySQL. However, future expansion of Windows Azure will enable support of multiple languages and frameworks, such as, Ruby on Rails, Python and so on. Further, applications deployed can use Web and Worker Role instances together for the user load. Multiple Web and Worker role instances can be configured using the service configuration file. One point to remember is that Windows Azure further provides a capability to retain the VMs where any crash leads to debugging and reusing the storage state to investigate the causes of the crash.[17]

The implementation of cloud can be done in many operating system but we have planned to increase security in cloud by implementing it in Microsoft Azure.

Table 2: Azure Comparison Chart [25]



Feature	Amazon EC2	Google AppEngine	Microsoft Azure
Cloud Service Areas	Infrastructure as a service	Platform as a service	Platform as a service
Compute Capability	64-bit platform, with four virtual core 2 EC2 compute units – supports multiple operating systems	Not disclosed	Comes with multiple configurations with different VM instances capacity.
Storage Engine	Supports SimpleDB and a simple storage service	No storage – as Google APIs can connect with any open store	SQL Azure Storage: Table, Blobs and Queues SQL Azure Database SQL Azure Data Sync
Platform Services	Not available	Google Services	Windows Azure AppFabric Services Ex: Service Bus and Access Control
Programming Language Support	Supports multiple open source languages and Java, Oracle and .Net	Python and Django	.Net Languages, Java, Apache Tomcat, Ruby, PHP, C, C++, MySQL Support for native languages and full-trust execution
Asynchronous Communication	Simple Queue Service	Not supported	Queues in Windows Azure Storage
Development Tools	Not applicable – only provides virtual machines to create images of the server platform	Does provide editing, simulation and deployment tools.	Visual Studio is one of the IDE used for developing cloud-based projects using Microsoft technologies and other supporting languages.

In the cloud the server will first authenticate the person who is logging in to the cloud. If the person is authenticated it will ask whether it wants to upload or retrieve data present in the cloud. If the person wants to upload data into the cloud, the cloud server will allow the user to do so and when the user logs out of the cloud, the data will be automatically encrypted using 3DES by using the password as the key.

If the user wants to retrieve the data present in the cloud, the cloud will automatically decrypt the data in the original form which will be done by the same decryption technique using the same key and will be able to access his data as he is authenticated by the security key. The Figure 5 below shows the Architecture of Cloud.

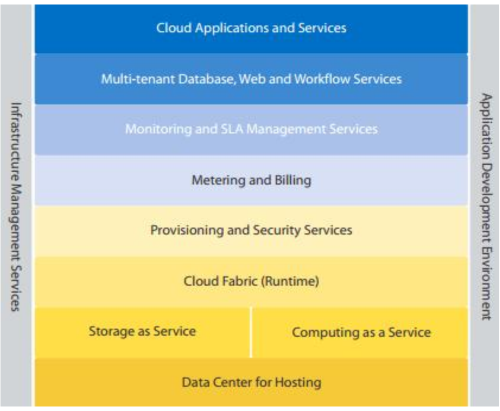

Cloud Applications and Services
Multi-tenant Database, Web and Workflow Services
Monitoring and SLA Management Services
Metering and Billing
Provisioning and Security Services
Cloud Fabric (Runtime)
Storage as Service
Computing as a Service
Data Center for Hosting
Infrastructure Management Services
Application Development Environment

Figure 5. Architecture of Cloud [25]

2.7 DESIGN OVERVIEW

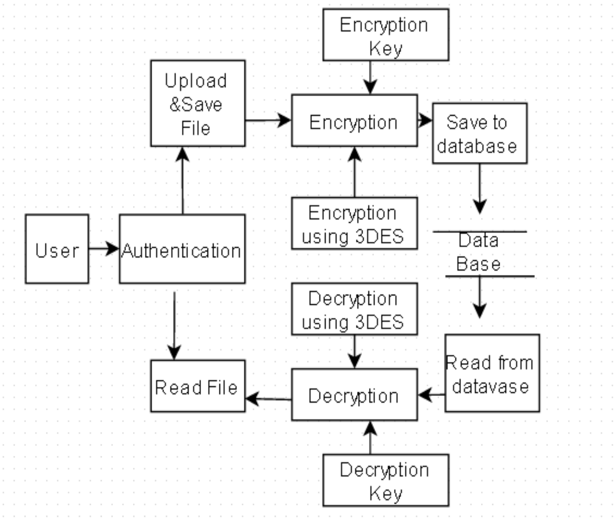


Figure 6. Block-Diagram

3. FUTURE WORK

To provide low-power processors and cheaper clouds. To improve the security by integrating more high level encryption techniques. In upcoming years we can add more security like when we are sending our data over the network from cloud the data will be sent in an encrypted form.

4. REFERENCES

[1] Priyanka Arora, Arun Singh, Himanshu Tyagi ―Analysis of performance by using security algorithm on cloud network‖ in international conference on Emerging trends in engineering and management (ICETM2012), 23-24 june, 2012.

[2] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication 800-144, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494, (2011) December.

[3] H. T. Dinh, C. Lee, D. Niyato and P. Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches", Wireless Communications and Mobile Computing – Wiley,http://www.eecis.udel.edu/~cshen/859/papers/survey_MCC.pdf.

[4] New Comparative Study Between DES, 3DES and AES

[5] within Nine Factors Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani

[6] "Definition of: SaaS". PC Magazine Encyclopedia. Ziff Davis. Retrieved 14 May 2014.

[7] "IT Channel Glossary". CompuBase. March 2013. Retrieved 13 February 2013.

[8] "Software as a Service (SaaS)". Cloud Taxonomy. Open crowd. Retrieved 24 April 2011.

[9] Brandon Butler, "PaaS Primer: What is platform as a service and why does it matter?" Network World, February 11, 2013.

[10] "Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS," Rackspace, October 22, 2013.

[11] William Y. Chang, Hosame Abu-Amara, Jessica Feng Sanford, "Transforming Enterprise Cloud Services", London: Springer, 2010, pp. 55-56.

[12] Wang, R. "Tuesday's Tip: Understanding The Many Flavors of Cloud Computing and SaaS". Retrieved 2012-05-27.

[13] Barker, William C.; Barker, Elaine (January 2012)." NIST Special Publication 800-67 Revision 1: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (PDF").

[14] According to ANSI X3.92-1981 (one of the standards that defines the DES algorithm), section 3.5: "One bit in each 8-bit byte of the KEY may be utilized for error detection in key generation, distribution, and storage. Bits 8, 16,..., 64 are for use in ensuring that each byte is of odd parity."

[15] Security and Privacy Issues in Cloud Computing Jaydip Sen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

[16] IDC (2009) Cloud Computing 2010 – An IDC Update. slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update

[17] "Security and Privacy Issues in Cloud Computing" Jaydip Sen, Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

[18] http://www.tcs.com/SiteCollectionDocuments/White%20Papers/HighTech_Whitepaper_Windows_Azure_09_2011.pdf

[19] International Journal of Scientific Engineering and Research (IJSER) www.ijser.in ISSN (Online): 2347-3878

[20] “Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System” Karthik .S1, Muruganandam,A2. Volume 2 Issue 11, November 2014 Licensed Under Creative Commons Attribution CC BY

[21] "SSO and LDAP Authentication". Authenticationworld.com. Retrieved 2014-05-23.

[22] "OpenID versus Single-Sign-On Server". alleged.org.uk. 2007-08-13. Retrieved 2014-05-23.

[23] "Biometrics: Overview". Biometrics.cse.msu.edu. 6 September 2007. Retrieved2012-06-10.

[24] Jain, A.; Hong, L. and Pankanti , S. (2000). ”Biometric Identification". Communications of the ACM, 43(2), p. 91–98. DOI 10.1145/328236.328110

[25] Jain, Anil K.; Ross, Arun *(2008).* "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2.

[26] Sahidullah, Md (2015). "Enhancement of Speaker Recognition Performance Using Block Level, Relative and Temporal Information of Subband Energies". PhD Thesis *(*Indian Institute of Technology Kharagpur).

[27] **“**Windows Azure – The Cloud Computing Platform” TCS white paper.