International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-2, February 2015

Security Issues In Cloud Computing and Solution to Resolve Them

Kimmi Makhija, Pawan Kumar

***Abstract*— Cloud computing refers to providing computing and communications–related services with the aid of remotely located, network-based resources without a user of such resources having to own these resources. The network in question typically, though not necessarily, is the Internet. The resources provisioned encompass a range of services including data, software, storage, security, and so on. For example, when we use a mail service such as Gmail, watch a movie on YouTube, shop at Amazon.com, or store files using Drop Box, we are using cloud-based resources (The Google Chrome Team, 2010). In this paper, we will explain definitions and various security challenges associated with the use of cloud services and propose a layered approach of security measures that the organization can undertake to manage the risks associated with the use of cloud computing. This paper observes approaches to algebraic analysis of GOST 28147-89 encryption algorithm (also known as simply GOST), which is the basis of most secure information systems in Russia.**

***Index Terms*— CSA, Gartner, Iaas, Paas, Saas**

I. INTRODUCTION

In the field of computation, there have been many approaches for enhancing the parallelism and distribution of resources for the advancement and acceleration of data utilization. Data clusters, distributed database management systems, data grids, and many more mechanisms have been introduced. Now cloud computing is emerging as the mechanism for high level computation, as well as serving as a storage system for resources. Cloud primarily refers to saving of user's data to an offsite storage system that is maintained by a third party. This means instead of storing information on user computer's hard disk or other storage devices, client save it to a remote data base where internet provides the connection between user computer and the remote data base. Computers in the cloud are configured to work simultaneously and the various applications use the collective computing power as if they are running on a cloud using the concept of virtualization .In this model customer's plug into the cloud to access information technology resources which are priced and provided on-demand. Essentially, IT resources are rented and shared among multiple tenants like office space, apartments or storage spaces are used by tenants .Delivered over an internet connection, the cloud eliminates the company's data center or server.

Cloud computing is independent computing it is totally different from grid and utility computing. Google Apps is the paramount example of Cloud computing, it enables to access services via the browser and deployed on millions of machines over the internet. Resources are accessible from the cloud at any time and from any place across the globe using the internet. Cloud computing is cheaper than other computing models; zero maintenance cost is involved since the service provider is responsible for the availability of services and clients are free from maintenance and management problems of the resource machines.

Cloud computing provides enterprises the capability to deliver IT resources in a way that can be scaled dynamically to address customers ever changing requirements. Key benefits to the enterprise are the reduction of investment and maintenance cost however, with the great potentials offered by the cloud, it also comes with the security issues. Since the computation and storage of data are on the cloud, outside the enterprises' datacenter, there are greater risks of data leakage and cyber-attack by hackers. The adoption of cloud computing may move quite quickly depending on local requirements, business context and market specificities. We are still in the early stages, but cloud technologies are becoming adopted widely in all parts of the world. The economic potential of cloud computing and its capacity to accelerate innovation are putting business and governments under increased pressure to adopt cloud computing-based solutions.

1.1 Types of Clouds

Public: In public cloud (also known as external cloud), the services are provided by a third party via Internet, and they are available and are for commercial purposes.

Private: This cloud consists on the hosting of private applications and services for private use (private networks) only.

Hybrid: It's a combination of public and private cloud. This is a better option when someone don't want to invest too much in infrastructure and on the other side wants the data to be secured by using private cloud deployment.

Community: A community cloud is an infrastructure shared by several organizations which supports a specific community.

1.2 Literature review

Cloud computing is a latest buzz in information technology era which shifts computing resources and data away from traditional backend servers on to data centers. Basically applications, storages, databases and various IT services are delivered as a service over the Internet. Presently many very large companies are part of the cloud service development and offering examples are Microsoft, IBM, Amazon and Google.

Manuscript received February 13, 2015.

Kimmi Makhija: IT Department, Exfaculty of KIRAS (Affiliated to GGSIP University) Gandhi Nagar, Delhi- 31, 9873307773

Pumar Kumar: IT analyst in Tata Consultancy Services (TCS), Gandhi Nagar, Delhi-31, 9873307773

Although there is no definitive definition for cloud computing, a definition that is commonly accepted is provided by the United States National Institute of Standards and Technologies (NIST):

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

1.3 Existing Work on Cloud Security Guidance or Frameworks

In the few years since cloud computing arrived as a new model for IT, several efforts have already taken place to offer guidance for cloud security. These include:

- Cloud Security Alliance (CSA) The CSA has been very active in various efforts, including:
- Cloud Controls Matrix (CCM) This is "designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The Cloud Controls Matrix provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains."
- Consensus Assessments Initiative Questionnaire This effort is "focused on providing industry-accepted ways to document what security controls exist in IaaS, PaaS, and SaaS offerings, providing security control transparency."
- Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 published in December 2009 presented security guidance for a number of areas in cloud computing; these include architecture, governance, traditional security, and virtualization.
- Domain 12: Guidance for Identity & Access Management V2.1 published in April 2010 discusses the major identity management functions as they relate to cloud computing. This work forms a cornerstone of the CSA's Trusted Cloud Initiative.
- CloudAudit Seeks to give cloud adopters and cloud operators the tools to measure and compare the security of cloud services. It does this by defining "a common interface and namespace that allows cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance (A6) of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments."3
- European Network and Information Security Agency Leading the security guidance efforts in Europe, ENISA has produced several guiding publications for securely adopting cloud computing, these include:
- Cloud Computing: Information Assurance Framework Published in November 2009. Presents a set of assurance criteria that address the risk of adopting cloud computing.
- Cloud Computing: Benefits, Risks and Recommendations for Information Security Published in November 2009.
- The Federal CIO Council's Proposed Security Assessment and Authorization for U.S. Government Cloud Computing.4 The core importance of this document is that it adopts the NIST 800-53R3 security controls for cloud computing in low- and moderate-risk systems.
- The Trusted Computing Group (TCG) In September 2010, the TCG formed the Trusted Multi-Tenant Infrastructure Work Group, which is intended to develop a security framework for cloud computing. The Trusted Multi-Tenant Infrastructure Work Group will use existing standards to define end-to-end security for cloud computing in a framework that can serve as a baseline for compliance and auditing.

All of these efforts are relatively new and have yet to gain broad acceptance. More so, they are either initial activities that are intended to serve as a starting point for more formal work or the product of community efforts toward a common framework for cloud security. In other words, there is a great deal of uncertainty in this area. That presents a difficulty for cloud adopters who need to evaluate the security of their private or community clouds and also for users who need a means to evaluate the security of a cloud service.

Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing as depicted in figure1.

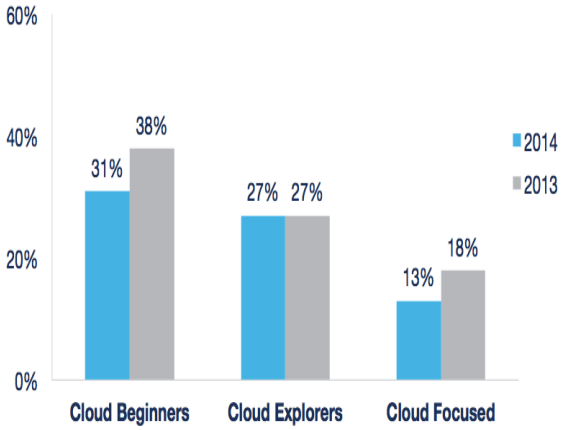

Figure 1: Respondents that see cloud security as a significant Challenge

1.4 SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing promises to significantly change the way we use computers and access and store our personal and business information With these new computing and communications paradigms arise new data security Challenges .Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. Data theft attacks are amplified if the attacker is a malicious insider. This is

considered as one of the top threats to cloud computing by the Cloud Security Alliance (CSA).

The Twitter incident is one example of a data theft attack from the Cloud. Several Twitter corporate and personal documents were ex-filtrated to technological website Tech Crunch, and customers'accounts, including the account of U.S. President Barack Obama, were illegally accessed. The damage was significant both for Twitter and for its customers. While this particular attack was launched by an outsider, stealing a customer's admin passwords is much easier if perpetrated by a malicious insider. Rocha and Correia outline how easy passwords may be stolen by a malicious insider of the Cloud service provider. According to a poll at Gartner's Data Center Conference in 2013, the No. 1 issue slowing adoption of public cloud computing is security and privacy, notably lack of confidence in the CSP's security capability. Here I am going to discuss some security issues:

According to Gartner, below listed are the seven security issues for cloud computing:

1) Privileged user access: Sensitive data processed outside the enterprise brings with it an inherent level of risk because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs.

2) Regulatory compliance: Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security.

3) Data location: When clients use the cloud, they probably won't know exactly where their data are hosted. Distributed data storage is a usual manner of cloud providers that can cause lack of control.

4) Data segregation: Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure Encryption and decryption is a classic way to cover security issues but heretofore it couldn't ensure to provide perfect solution for it.

5) Recovery: If a cloud provider broke or some problems cause failure in cloud sever what will happen to any data? Can cloud provider restore data completely? Moreover clients prefer don't get permission to third-party companies to control their data. This issue can cause an impasse in security.

6) Investigative support: Cloud services are specially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set.

7) Long-term viability: Ideally, cloud computing provider will never go broke or get acquired by a larger company with maybe new policies. But clients must be sure their data will remain available.

CSA indicates that the report reflects the consensus of the experts on the most significant threats to security in the cloud and focuses on the threats arising from the sharing of common resources. The report is intended to help users of the cloud and cloud services providers to implement the best strategies to reduce risk.

1) Data Theft

Theft of confidential corporate information is always a risk to any IT infrastructure, but CSA indicates the cloud model offers new, major highways attacks. If the base of the cloud data from multiple leases is not thought out properly, a flaw in the application of one client can open attackers' access to data not only of the client, but all other cloud users.

2) Loss of Data

The data stored in the cloud, can be stolen by hackers or lost for other reasons, says CSA. Data can suffer a fire or natural disaster or data can be accidentally deleted if a provider of cloud services does not introduce proper backup measures. On the other hand, the customer, which encrypts the data before upload them to the cloud, suddenly lost the encryption key, adds CSA.

3) Service Traffic Hijacking

In a cloud environment attacker could use the stolen login information to intercept, forge or give distorted information to redirect users to malicious sites, says CSA. Organizations should prohibit distribution of their login information for all services. CSA recommends a robust, two-factor authentication to reduce the risk.

4) Insecure Interfaces and API

Organization is subjected to a variety of threats if they use weak interface software or API to manage and interact with cloud services. These interfaces must be well designed and secured to include authentication, access control and encryption.

CSA adds that organization and third-party contractors often use cloud interfaces to provide additional services, making them more complex and increases the risk, as it may require that the customer told their registration data to such contractor to facilitate the provision of services.

5) Denial of Service

The cloud can be made attacks such as denial of service that cause an overload of infrastructure, making use a huge amount of system resources and not allowing customers to use the service. Media attention often involve distributed, or DDoS-attacks, but there are other types of DoS-attacks, which can block the cloud usage.

For example, attackers can launch DoS-attacks on asymmetric application layer by exploiting vulnerabilities in the Web-servers, databases, or other cloud resources to fill up the application with a very small payload.

6) Malicious Insiders

CSA warns without proper level of security on IaaS, PaaS or SaaS, an insider who has improper intentions (e.g., system administrator) may gain access to confidential information that it is not intended for him.

Malicious insiders are certified to do greater and bigger damage than any other attacks. According to CSA, even if encryption is implemented, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack.

For securing data in cloud computing, cryptographic encryption mechanisms are certainly the best options. Encryption is the best option for securing data in transit as well. In addition, authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit.

II. ENCRYPTION ALGORITHM

There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more

cipher texts would be unable to decipher the cipher text or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt cipher text or discover the key even if he or she is in possession of a number of cipher texts together with the plaintext that produced each cipher text.

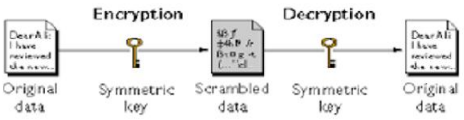

Figure 2: Symmetric-key Encryption

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

There have been many discussions on different algorithms (i.e. AES, 3DES, RSA etc.) in various papers to provide data security in cloud computing. Below is the explanation of one of the best algorithms (developed by Russia) to provide data security:

2.1 GOST ALGORITHM:

The GOST algorithm is a symmetric block cipher developed by the Russian government. GOST is the acronym for Gosudarstvennyi Standard in Russian, whose English equivalent is Government Standard. The Government Standard of the USSR 28147-89, Cryptographic protection for Data Protection Systems, appears to have played the role in the former Soviet Union (not only in Russia) similar to that played by the US Data Encryption Standard (FIPS 46).The GOST encryption algorithm is a state encryption standard in Russian Federation. The GOST 28147-89 algorithm is recommended by the Federal Security Service of Russia for building cryptographic protection systems for data of limited distribution (commercial secrets, personal data, etc.) Any cryptographic system of data protection certified by the Federal Security Service has to be built using only the following algorithms: GOST R 34.10-2001, GOST R 34.11-94, GOST 28147-89. That is why the majority of information systems for confidential data protection are based on GOST 28147-89.

Originally, the algorithm became known to the international community in 1994 when it was declassified and translated into English. Despite the fact that GOST was designed more than 20 years ago, in 2010 it was among the candidates for codification as an international encryption standard as ISO 18033. At the session of the 27th ISO committee in 2010, a decision was made to initiate inclusion of GOST into the international standard ISO/IEC 18033.3The first version was prepared in January, 2011. However, in February 2011 a presentation was made at Fast Software Encryption (FSE) symposium.

As of January 27th 2012, the addendum on GOST 28147-89 was deleted from ISO/IEC 18033-3. The Russian party proposes to continue negotiations on considering GOST algorithm as an international standard and to proceed to the second version of proposals. Based on the publications mentioned above, one can make a conclusion that in order to make the decision about inclusion of GOST into ISO/IEC 18033.3, further research on its cryptographic strength should be carries out. The GOST 28147-89 standard includes output feedback and cipher feedback modes of operation, both limited to 64-bit blocks, and a mode for producing message authentication codes.

GOST encryption has four operation modes: simple substitution mode, stream mode, stream mode with feedback and authentication mode. Simple substitution mode is the basic one and all other modes contain it in their structure. We will consider only this mode in this paper. The GOST algorithm takes an input of 64-bit data blocks and uses the cipher key K of length 256-bits to encrypt or decrypt plain text or cipher text. The given cipher key is divided into eight subkeys, each 32-bits, that are represented as K_1, K_2, K_3, ..., K_8. The GOST algorithm performs its processing by repeating a simple algorithm for 32 iterations; each iteration uses a different subkey.

The steps of the GOST encryption process are:

1. Select a plain text M.
2. Split the plain text M into two halves and represent them as L0 and R0.
3. Initialize the value of the variable i with 1.
4. Assign the value of Ri-1 to Li
5. Perform the process of modulo 232 addition on the right half, R, and a subkey Ki. A list of subkeys is used in the GOST algorithm for each iteration.

   Table B-1 shows the subkeys in each iteration of the GOST encryption process:

Table B-1: Subkeys in the GOST Encryption Process

Iteration	Subkey Used
1	K_1
2	K_2
3	K_3
4	K_4
5	K_5
6	K_6
7	K_7
8	K_8
9	K_1
10	K_2
11	K_3
12	K_4
13	K_5
14	K_6

Table B-1: Subkeys in the GOST Encryption Process

Iteration	Subkey Used
15	K_7
16	K_8
17	K_1
18	K_2
19	K_3
20	K_4
21	K_5
22	K_6
23	K_7
24	K_8
25	K_8
26	K_7
27	K_6

Table B-1: Subkeys in the GOST Encryption Process

Iteration	Subkey Used
28	K_5
29	K_4
30	K_3
31	K_2
32	K_1

6. The output of step 5 is further split into groups of 4 bits. You can get eight such groups.
7. Each of the groups is searched in the corresponding S-boxes to get an output that corresponds to the input. S-boxes contain numbers from 1 to 15 that are arranged in a permutation.

   Table B-2 shows the S-boxes used in GOST algorithm:

Table B-2: S-Boxes Used in GOST Algorithm

S-box 1															
4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3
S-box 2															
14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9
S-box 3															
5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11
S-box 4															
7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3
S-box 5															
6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2
S-box 6															
4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
S-box 7															
13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
S-box 8															
1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

   For example, when the input to the first S-box is 0, then the output is 4, whereas, when the input is 2, the output is 2.
8. The output from the S-blocks is combined to form the 32-bit word.
9. Shift the 32-bit word to the left by 11 bits.
10. Perform the XOR operation on the result of step 9 and left half of the text, and assign it to the new right half that R_{i+1} denotes.
11. Assign this new right half to the left half.
12. Increment the value of i by 1.
13. Repeat step 4 to step 11 until the value of i = 33.

At the end of the encryption process, concatenate the values of L_{32} and R_{32} to generate the cipher text. The steps of the GOST decryption process are the same as the encryption process with the order of subkey ki reversed.

III. SUMMARY

Cloud Computing is revolutionizing the way business is carried out in various industries (Government, Healthcare, and Software etc), use of information technology resources and services, but the revolution always comes with new problem. One of the major problems associated with cloud computing is security. Various security issues and algorithm to deal with data security issues are discussed in multiple papers. This paper discusses various security issues according to Gartner, CSA and one of the solution to resolve them.

ACKNOWLEDGMENT

I express my deep gratitude and sincere thanks to my husband **Mr. Pawan kumar Makhija , MCA (IT analyst in Tata Consultancy Services(TCS))** for his valuable, suggestion, innovative ideas, constructive, criticisms and

inspiring guidance had enabled me to complete the work successfully.

REFERENCES

[1]Security Attacks and Solutions in Clouds ,Kazi Zunnurhain and Susan V. Vrbsky,Department of Computer Science ,The University of Alabama,Tuscaloosa, AL 35487-0290 ,kzunnurhain@crimson.ua.edu, vrbsky@cs.ua.edu.

[2] JOURNAL OF NETWORK AND COMPUTER APPLICATION: A combined approach toensure data security in cloud computing BY Sandeep K.Sood Department of Computer Science and Engineering ,GNDU ,Regional Campus Gurdaspur(Punjab)247667,India.

[3] Security, Trust, and Regulatory Aspects of Cloud Computing in Business Environments by S. Srinivasan (ed) IGI Global © 2014 (325 pages) *Citation* ISBN:9781466657885.

[4] Privacy and Security for Cloud Computing by Siani Pearson and George Yee (eds) Springer © 2013 (312 pages) *Citation* ISBN:9781447141884.

[5]Security Threats in Cloud Computing:Engr: Farhan Bashir Shaikh Department of Computing & Technlogy SZABIST Islamabad, Pakistan Shaikh.farhan@live.com ;Sajjad Haider IT Department NUML Islamabad, Pakistan Sajjadhyder@hotmail.com

[6]https://robiulislam.wordpress.com/2011/12/28/cloud-computing-security/

[7]International Journal of Engineering and Technical Research (IJETR); ISSN: 2321-0869, Volume-2, Issue-11, November 2014

Distributed Versus Cloud Computing and data; security issues and new trends- Fog Computing; Sachin R. Desale, Kadambari V. Vanmali, Brajendra Singh Rajput.

[8]CRYPTOGRAPHY AND NETWORK SECURITY *PRINCIPLES AND PRACTICE* FIFTH EDITION William Stallings Prentice Hall; Boston Columbus Indianapolis New York San Francisco; Upper Saddle River Amsterdam Cape Town Dubai London Madrid ;Milan Munich Paris Montreal Toronto Delhi Mexico City Sao Paulo; Sydney Hong Kong Seoul Singapore Taipei Tokyo

[9]cryptography Protocols and Algorithms : Skill soft Press © 2003 (100 pages)

[10] Journal of Computer and Communications, 2, 10-17. http://dx.doi.org/10.4236/jcc.2014.24002; A Algebraic Cryptanalysis of GOST Encryption Algorithm: Ludmila Babenko, Ekaterina Maro; Department of Information Security, Southern Federal University, Taganrog, Russia

[11] http://www.jetico.com/web_help/bc8/index.php?info=html/02 basic concepts/05 encryption algorithms.htm

[12] Theory and Practice of Cryptography Solutions for Secure Information Systems by Atilla Elçi (ed) et al. IGI Global © 2013 (611 pages) *Citation*:ISBN:9781466640306;

[13] http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2014-state-cloud-survey

[14] CSA-GRC-Stack-v1.0-README.pdf. http://www.cloudsecurityalliance.org/.

[15] Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, Draft version 0.96, CIO Council, US Federal Government; 2010.

[16] Securing the Cloud: Cloud Computer Security Techniques and Tactics by Vic (J.R.) Winkler; Syngress Publishing © 2011 (315 pages) Citation; ISBN:9781597495929

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

[18] Advance in Electronic and Electric Engineering. ISSN 2231-1297, Volume 4, Number 4 (2014), pp. 425-428 © Research India Publications http://www.ripublication.com/aeee.htm Well-known Gartner's Seven Security Issues Which Cloud Clients Should Advert

[19] http://blogs.gartner.com/security-summit/announcements/assessing-the-top-risks-for-public-cloud/

Kimmi Makhija - I have 3+ years of experience as an assistant professor with GGSIP University. My highest qualification is MCA (from MDU) and I started my teaching carrier in 2010. I had published paper on “A study of SQL injection in banking transaction” in international journal of engineering inventions (IJEI).

Pawan Kumar - I have 7+ years of experience in software design, development and testing, currently working as IT analyst with TCS. My highest qualification is MCA (from UPTU) and I started my IT carrier with HCL technologies in 2007