International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Analysis of Security of Cloud with Encryption by Utilizing Symmetric and Asymmetric Algorithm

Prof. Satish Soni[1], Pragati Gupta[2]

[1]Professor & Head of Computer Science & Engineering Department, JNCT Rewa M.P. 486001 India
[2]Scholar, Computer Science & Engineering Department, JNCT Rewa M.P. 486001 India

ABSTRACT:

In the cloud environment, resources are shared between all the servers, users and individuals. So, it is complex for the cloud provider to ensure file security. Also, if communications are not encrypted or shielded, password or other important flow of information can be at risk over transmission. Unsecured cloud environment, is very easy for an intruder to access, misuse and destroy the original form of data. In case of compromise at any cost; entrusting cloud is of no use. A need for "practically strong and infeasible to get attacked" technique becomes vital. The paper presents the file security model which uses the concept of hybrid symmetric and asymmetric encryption algorithm scheme to meet security needs. Here, we are conducting research on secure and safe cloud computing and practice. At present, due to the extensive complexity of the cloud, we accept that it will be almost impossible to provide a complete and holistic solution to securing the cloud. Therefore, our aim is to suggest incremental enhancements towards securing the cloud that will eventually result in a secure cloud storage and environment.

1. Introduction

1.1 Introduction to security in Cloud

There is a strong & critical requirement to securely store, manage, share and analyses huge amounts of complex data to determine patterns and trends. Because of the critical nature of the businesses, it is important that clouds are secure. If someone wants to gain from the benefits of using cloud computing, one must also utilize the resource allocation and scheduling provided by clouds. This leads to the biggest security challenge with clouds where the owner of the data does not have control on whereabout of the data. Therefore, we need to safeguard the data during untrusted processes.

1.2 Cloud computing service models

As per the definition of NIST [1], there are 3 types of service models in cloud computing

1.3.1 SaaS

SaaS stands for Software as a Service. It provides users the capability to host their application/software on the cloud infrastructure. Application can be accessed through a web interface such as browsers like google chrome, Internet explorer etc.

1.3.2 PaaS

PaaS stands for Platform as a Service. It provides users capability to deploy application on cloud platform instead of installing on local user system. It provides a platform layer on cloud infrastructure. SDKs, OS, APIs are some examples which can be deployed as PaaS.

1.3.3 IaaS

IaaS stands for Infrastructure as a Service. It provides consumers capabilities to host services like server, processing power, storage service and/or database on cloud infrastructure. Users can run required software's/applications or OS.

1.4 Cloud Computing Deployment Models

It has 4 types of deployment models ,

Public Clouds

In public cloud vendors dynamically allocate resources on a per-user basis through web applications. For example: Drop Box, SkyDrive and Google drive

Private Cloud

Due to security and availability issues more and more companies are choosing Private Clouds. It provides more secure platform to the employees and customers of an organization. For example, Banks, in banks all the employees and customers can access the bank data which is assigned to them particularly.

Hybrid Cloud

It is a blend of the of the Public & Private cloud. In hybrid cloud system, the internal resources, stays under the control of the customer, and external resources delivered by a cloud service provider.

Community Cloud

The community cloud shares the infrastructure around several organizations which can be managed and hosted internally or by third party providers.

2. Literature Review

Brian Hay et. al [1] have focused on data querying, data integrity, data authentication, and outsourcing of the encrypted data. Their research says that, the risks can rise at operational trust modes, or at resource sharing, or by formulating new attack strategies. In the operational trust modes, the channels are fully encrypted for communication are used for cloud storage and to perform process and computation on encrypted data which is termed as homomorphic encryption [6]. Virtual Machine Introspection (VMI) can be used at virtualization layer to process, compute and manipulate the data, it is one of the newest attack strategies.

Kevin Curran et.al [2] mentioned that Cloud Computing has a distributed architecture that consolidates server resources on a platform to provide on demand computing services and power. Cloud computing has become a flexible platform for organizations and companies to build their IT infrastructures. If companies desire to take advantage of cloud based IT systems by storing their data in Cloud Storage and perform computation on cloud, they will face the task of seriously reassessing their current security strategy.

Sanjoli Singla and Jasmeet Singh[3] also presented Cloud computing security using encryption technique: In this paper, data security during data transmission is dealt by both the authors. The main concern here is data encryption so that data confidentiality and its privacy can be attained. The algorithm used here is EAP- CHAP along with Rijndael Encryption Algorithm (RES).

3: Survey

3.1 Introduction to cloud security Issues & Dependencies

As per Venshila SanthaKumar, Jeno Lovesum" Survey on Data Security in Cloud Computing Using Combined Approach" [18], businesses and researchers across all industries conduct surveys to uncover answers to specific, important questions. These questions are varied, cover a diverse range of topics, and can be asked in multiple formats. Your questions should be strategically planned and structured in the best way possible to receive the most accurate data.

When structuring your survey questions, consider the following:

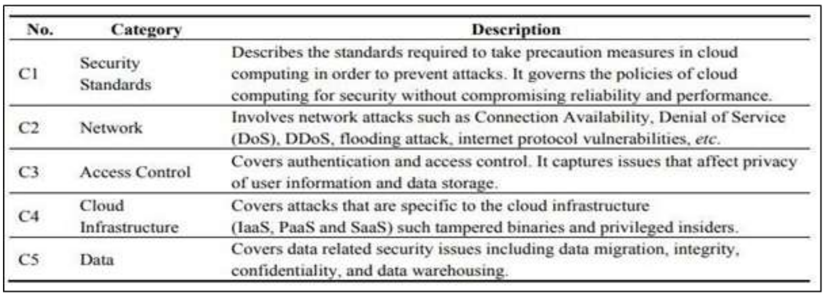
- The main goal
- How you plan to apply the survey data
- The decisions you will make because of the survey data

3.2 Categories and Issues

We have classified cloud computing security related issues into 5 categories, which are also list in Table 1.

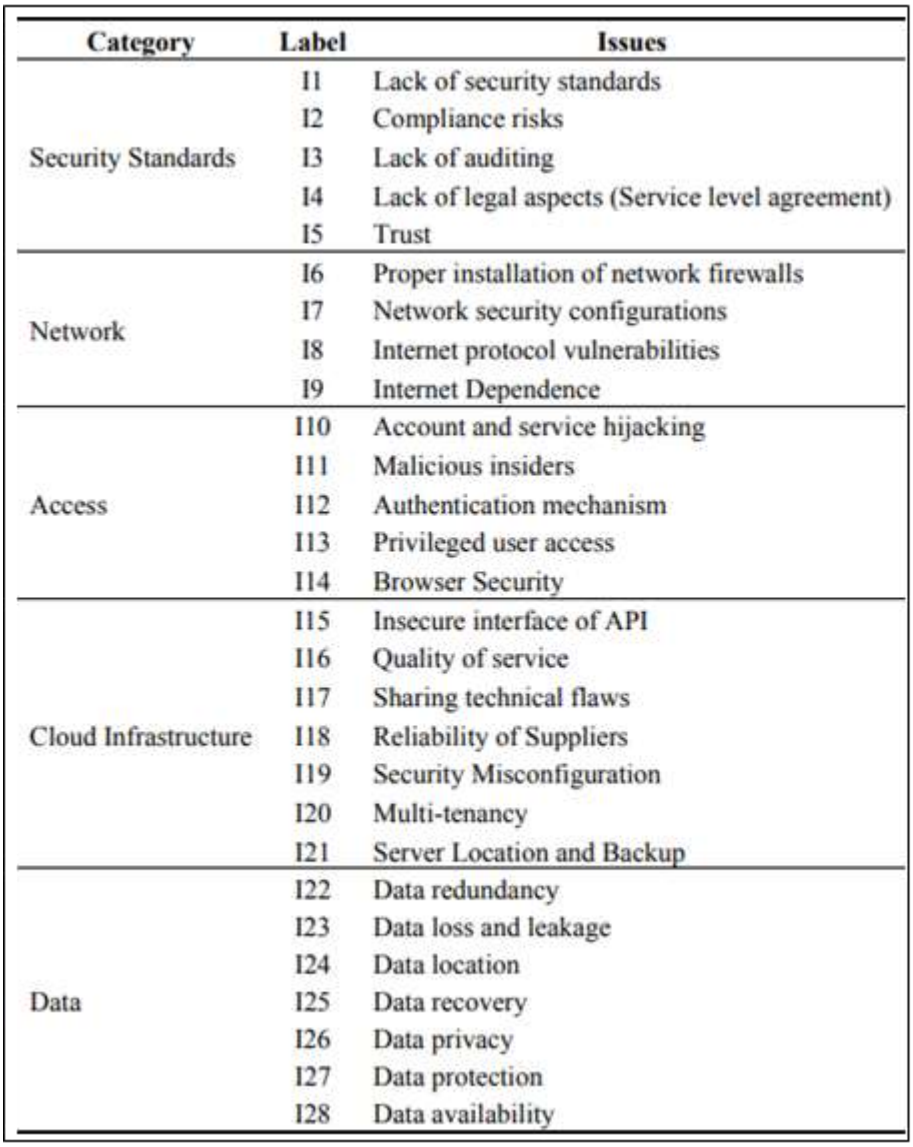
1. C1, The Security Standards – It deals with supervisory establishments and governing bodies that define cloud-security policies to make sure secure working environment over the clouds is available always. It includes SLAs, audits and other contracts among cloud users, cloud computing service provider and miscellaneous stakeholders.
2. C2, The Network- Refers to the medium using which the users connect to cloud infrastructure to perform actions and computations. It includes web- browsers, network connections and information exchange.

3. C3, The Access Control- It is a user related category and includes authentication and authorization issues.
4. C4, The Cloud Infrastructure- It includes problems within SaaS, PaaS and IaaS and is mostly related with environment.
5. C5, Data - covers data confidentiality and integrity issues.



No.	Category	Description
C1	Security Standards	Describes the standards required to take precaution measures in cloud computing in order to prevent attacks. It governs the policies of cloud computing for security without compromising reliability and performance.
C2	Network	Involves network attacks such as Connection Availability, Denial of Service (DoS), DDoS, flooding attack, internet protocol vulnerabilities, *etc*.
C3	Access Control	Covers authentication and access control. It captures issues that affect privacy of user information and data storage.
C4	Cloud Infrastructure	Covers attacks that are specific to the cloud infrastructure (IaaS, PaaS and SaaS) such tampered binaries and privileged insiders.
C5	Data	Covers data related security issues including data migration, integrity, confidentiality, and data warehousing.

Table 3.1 Categories of Cloud Computing security issues



Category	Label	Issues
Security Standards	I1	Lack of security standards
	I2	Compliance risks
	I3	Lack of auditing
	I4	Lack of legal aspects (Service level agreement)
	I5	Trust
Network	I6	Proper installation of network firewalls
	I7	Network security configurations
	I8	Internet protocol vulnerabilities
	I9	Internet Dependence
Access	I10	Account and service hijacking
	I11	Malicious insiders
	I12	Authentication mechanism
	I13	Privileged user access
	I14	Browser Security
Cloud Infrastructure	I15	Insecure interface of API
	I16	Quality of service
	I17	Sharing technical flaws
	I18	Reliability of Suppliers
	I19	Security Misconfiguration
	I20	Multi-tenancy
	I21	Server Location and Backup
Data	I22	Data redundancy
	I23	Data loss and leakage
	I24	Data location
	I25	Data recovery
	I26	Data privacy
	I27	Data protection
	I28	Data availability

Table 3.2 Cloud security Issues and classifications

4: Result and its Analysis

4.1 Introduction

Outcome of the SLR process and conducted survey is presented in this section of the report. We recognized safety trials and moderation methods from SLR by the analysis of results and given data about review participants and clarified the studied consequences from the study.

4.2 SLR Results

Cloud computing originated in 2006 but major papers [35] and researches were published after 2010. The articles considered in our research range of time from 2010 to 2017. Studies were identified for this research. Impact factors and no of citations are considered for this report. Articles from late 2017 and 2018 are not considered as they are too recent for to be used to reference.

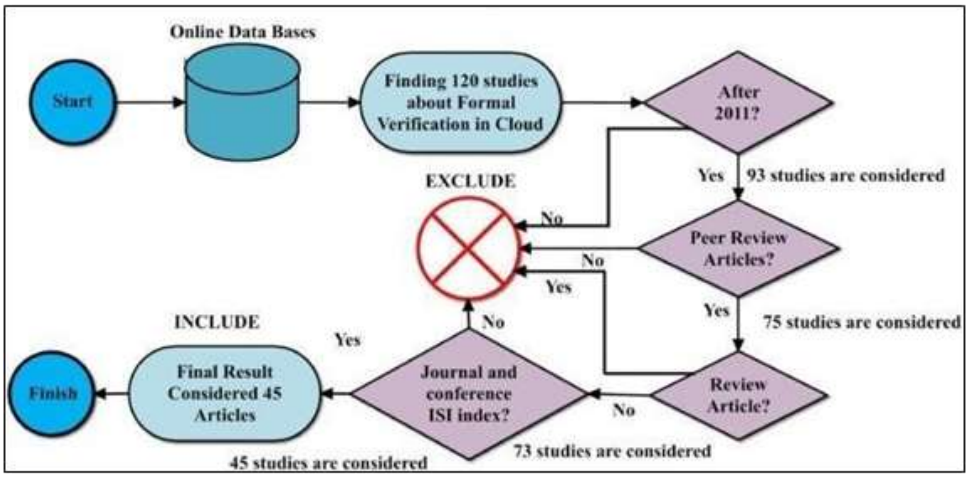

Online Data Bases
Start
Finding 120 studies about Formal Verification in Cloud
After 2011?
Yes
93 studies are considered
EXCLUDE
No
Peer Review Articles?
No
Yes
Yes
75 studies are considered
INCLUDE
Yes
No
Review Article?
No
Finish
Final Result Considered 45 Articles
Journal and conference ISI index?
73 studies are considered
45 studies are considered

Figure 4.1: SLR based study selection

4.3 Survey Results

The survey identified the main impact of cloud computing will be on IT Pros over the next five years.

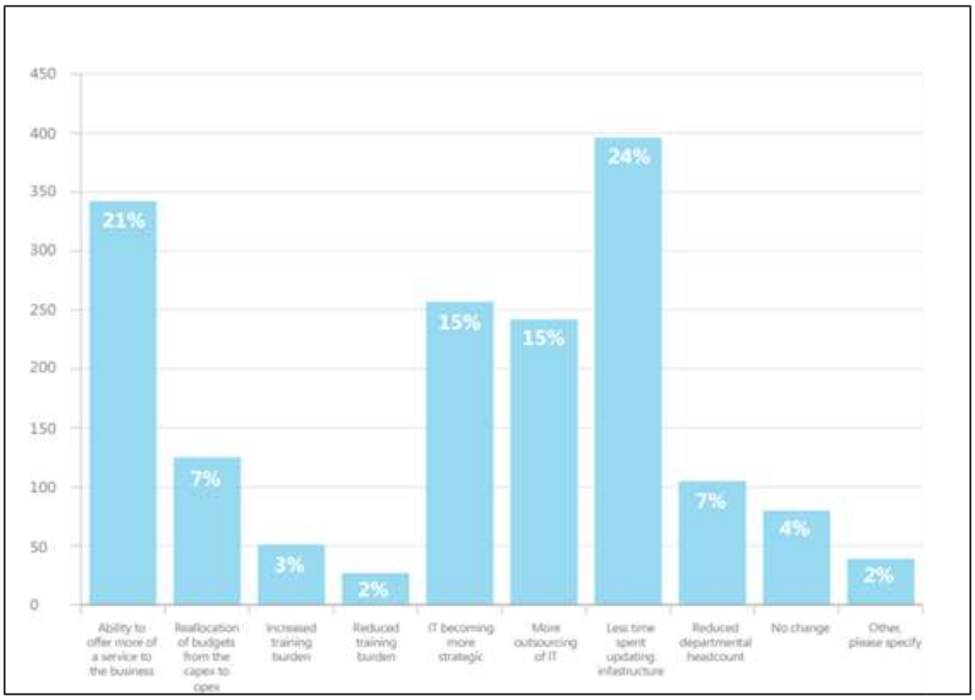


Figure 4.2: Survey Result of Impact of Cloud Computing

Then we identified the greatest barriers for adoption of the cloud in any organization:

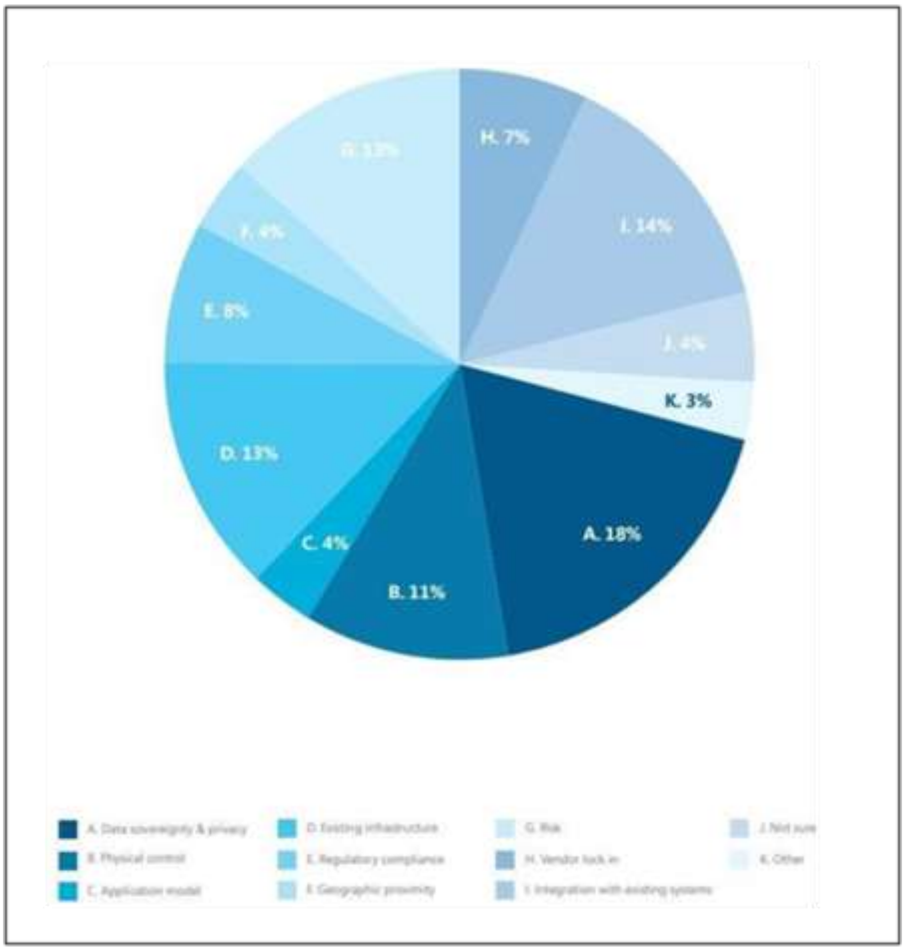

H. 7%
I. 14%
J. 4%
K. 3%
A. 18%
B. 11%
C. 4%
D. 13%
E. 8%
F. 4%
G. 13%
A. Data sovereignty & privacy
B. Physical control
C. Application model
D. Existing infrastructure
E. Regulatory compliance
F. Geographic proximity
G. Risk
H. Vendor lock in
I. Integration with existing systems
J. Not sure
K. Other

Figure 4.3: Barrier of Adoption

Total 17 Security challenges are identified through this survey. Summarized results are as follows:

1. High chances of security loss Eaves dropping
2. Attacks from viruses & malwares
3. Availability of Legal Interception point
4. Security arrangements for Virtual machine
5. Requirement of highly Trusted transaction
6. Risk due to presence of various and simultaneous Cloud users
7. Data sync from smart phone
8. Improper adaptation and use with proper risk assessment
9. Vulnerable APIs
10. Malicious insiders
11. Shared network
12. Service and traffic hijacking
13. Privacy -Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share common themes
14. Espionage- The use of spies by a government to discover the military and political secrets of other nations.
15. Business intelligence –It refers to technologies, applications and practices for the collection, integration, analysis, and presentation of business information. The purpose of Business Intelligence is to support better business decision making.

16. Data ownership – Data ownership is termed as having rights and control over all the data and survey elements. Owner should have legal and logical rights on the information. Distribution policy is completely controlled by the data owner.
17. Availability – The availability in system and solution architects, developers, and engineers with the knowledge needed to assess the impact of virtualization [41] and cloud computing on service reliability and availability. It reveals how to select the most appropriate design for reliability diligence to assure that user expectations are met.

The attributes which are compromised as a part of known challenges are as follows:

1. Confidentiality,
2. Security,
3. Availability and
4. Integrity.

Reported Mitigation Techniques

We have identified various security methods from this survey. Some of the mail security techniques are as follows:

SSL (Secure Socket Layer) Encryption

It works complete the usage of SSL records which cover an important pair and confirmed user identification data. When a Web customer links to a protect server resulting SSL protocols, the server shares a public key and exclusive session key with the client to create the encryption technique to be used for secure connection. All Cloud users and data should transact on encrypted carriers. Example: Optical fiber is a good means to transfer information, since fibers are harder to operate than electrical cables and are secure from normal penetration, cuts and breaks.

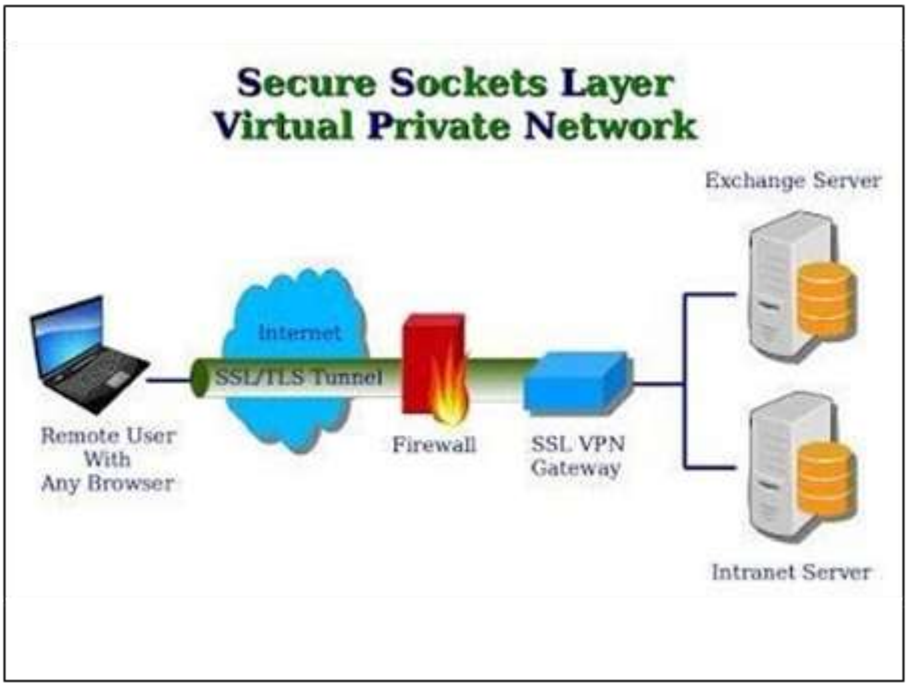


Figure 4.4: SSL VPN

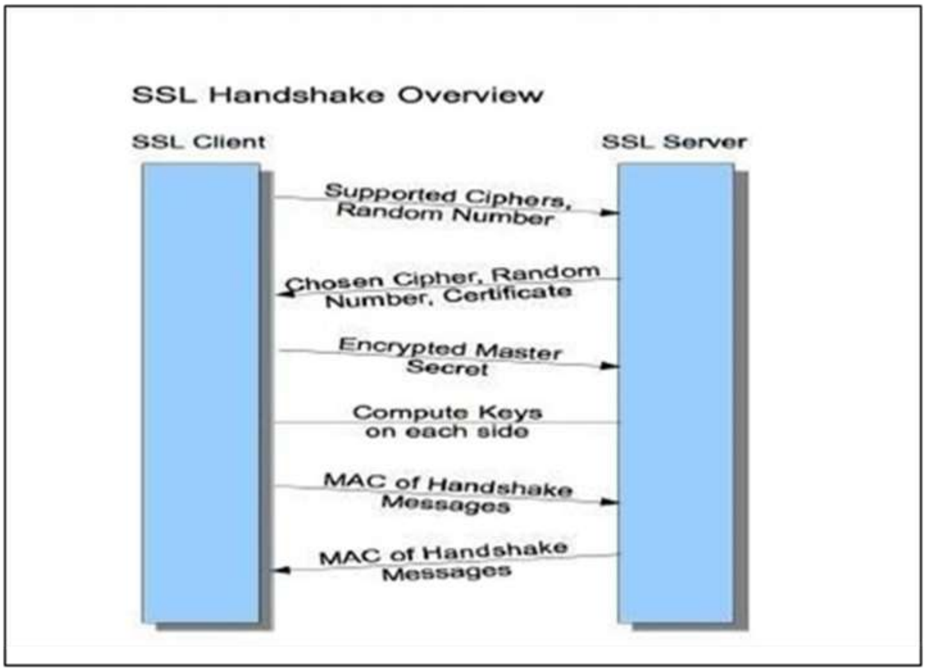

SSL Handshake Overview
SSL Client
SSL Server
Supported Ciphers, Random Number
Chosen Cipher, Random Number, Certificate
Encrypted Master Secret
Compute Keys on each side
MAC of Handshake Messages
MAC of Handshake Messages

Figure 4.5: SSL Handshake Overview

4.6 VPN (Virtual Private Network)

Virtual private networks (VPNs) provide the ability to create a secure network connection across a public network using encryption; thus, VPNs provide privacy and a level of trust. Before discussing the various trust, issues associated with VPNs, it's necessary to note that the term itself has multiple implementations. VPN types include network-to-network, multiple service host-server, to single-service host- server. Each of these implementations can be used in a cloud computing environment, and each has security strengths and weaknesses.

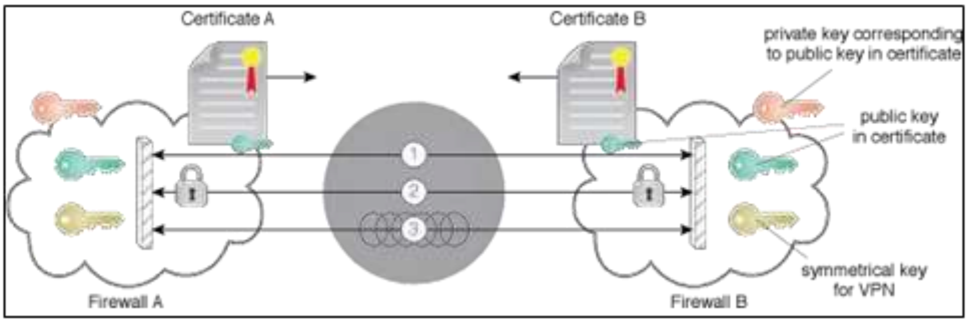

Certificate A
Certificate B
private key corresponding to public key in certificate
public key in certificate
1
2
3
symmetrical key for VPN
Firewall A
Firewall B

Figure 4.6: Firewall and Certificate over VPN

IPSec (Internet Protocol Security)

Internet Protocol security (IPSec) is a framework of open standards for helping to ensure private, secure communications over Internet Protocol (IP) networks using cryptographic security services. IPSec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. Because IPSec is integrated at the Internet layer (layer 3), it provides security for almost all protocols in the TCP/IP suite, and because IPSec is applied transparently to applications, there is no need to configure separate security for each application that uses TCP/IP.

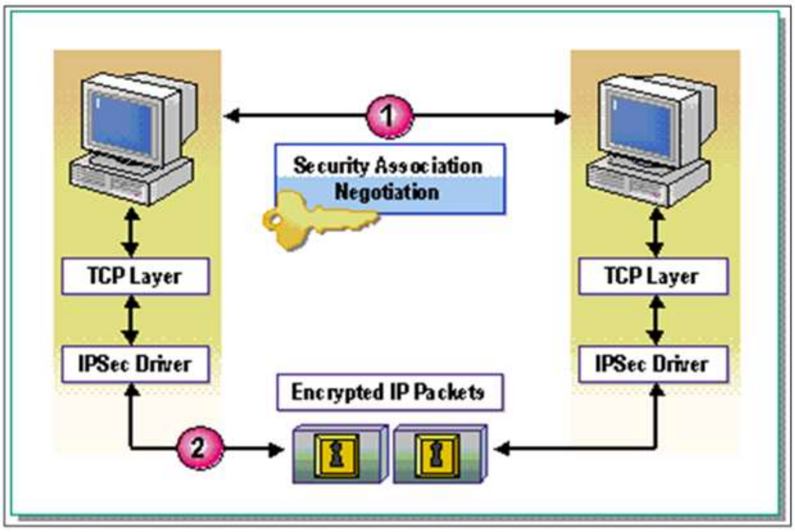


Figure 4.6: IPSec

IPSec helps provide defines-in-depth against:

- Network-based attacks from untrusted computers, attacks that can result in the denial-of-service of applications, services, or the network
- Data corruption
- Data theft
- User-credential theft
- Administrative control of servers, other computers, and the network.
- Encryption methods provide protection against eaves dropping.
- Encryption can handle active attacks and doesn’t let attackers go inside the cloud systems.
- Delay in response time from the cloud service provider could suggest a middle system monitoring activity which could be fatal in future.
- Auditing by 3rd party for security review.
- Kerberos, SSH and MD5 for authentication
- System Monitoring by Agent installed in client or provider system.
- Service management APIs

Privacy of Authentication data

Although an issue of paramount importance, little research has been carried out in this regard. Existing cryptographic techniques can be utilized for data security but privacy protection and outsourced computation need significant attention. Personal data should always remain in the user control, and the user decides what and whom they share their data with. Especially when implicit and context aware cloud authentication strategy is used, the identity provider needs access to real-time information about the user.

- Risk management.
- Standardization in security protocols.
- Destructive code should be handled with great efforts
- Cloud platform should be analyzed for security model.
- Strong authentication and ACLs.
- Good SCM (Supplier change management)
- Strong Access Point Interface control [31].
- Data protection across platform.
- Improved algorithms, 3rd party compliance, security strategy & good encryption techniques.

5. Conclusion

Large number of cloud services available pose a challenge to precise identification of security threats and challenges and its mitigation plans. Cloud fears largely stem from the perceived loss of control of sensitive data. Current control measures do not adequately address cloud computing's third-party data storage and processing needs. In approaches I present, the writers propose to extend control measures from the enterprise into the cloud using Trusted Computing and applied cryptographic techniques. These measures should alleviate much of today's fear of cloud computing, and, I believe, have the potential to provide demonstrable business intelligence advantages to cloud participation. cloud computing has the potential to be a disruptive force by affecting the deployment and use of technology.

The cloud could be the next evolution in the history of computing, following in the footsteps of mainframes, minicomputers, PCs, servers, smart phones, and so on, and radically changing the way enterprises manage IT.

REFERENCES

1. https://www.nist.gov/programs-projects/nist-cloud-computing-program- nccp
2. Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf, "NIST Cloud Computing Reference Architecture" US Department of Commerce, Gaithersburg, MD, 2017.
3. https://pdfs.semanticscholar.org/5696/d13ad3f552ab46769478cda611309 1edd888.pdf
4. Kevin Curran, Sean Carlin and Mervyn Adams, "Security issues in cloud computing", Elixir Network Engg.38 (2011), pp.4069-4072, August 2011.
5. Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847),Volume 3 Issue 3, pp.171-176, March 2014
6. Asphalting Judea, Kirti Modi, "c International Conference on Computing, Electronics and Electrical Technologies [ICCEET], 2017 IEEE.
7. P. Mell and T. Grace, "The nest definition of cloud computing, special publication 800-145," US Department of Commerce, Gaithersburg, MD, 2017.
8. Mohammad Sajid, Zahid Raza, "Cloud Computing: Issues & Challenges", International Conference on Cloud, Big Data and Trust 2017, RGPV.
9. Removing S, Eloff MM, Smith E, "The Management of Security in Cloud Computing", IEEE, 2017.
10. Bhaskar Prasad Rima, Eunji choir, Ian Lomb, "A Taxonomy and Survey of Cloud Computing System", IEEE 2016.
11. A Survey of Cryptographic Algorithms for Cloud Computing Rashmi Nigoti1, Manoj Jhuria2 Dr.Shailendra Singh3
12. A PROFICIENT MODEL FOR HIGH END SECURITY IN CLOUD COMPUTING. Source: ICTACT Journal on Soft Computing . Jan2014, Vol. 4 Issue 2, p697-702. 6p. Author(s): Chandar, R. Bala; Kavitha, M. S.; Seenivasan, K.