International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 07, July-2015

A Review on Security Threats and Vulnerabilities in Cloud Computing

G. Elavarasan
Research Scholar,
Department of Computer Science,
Karpagam University, Coimbatore
Tamilnadu, India.

Dr.S Veni,
Research Supervisor,
Department of Computer Science,
Karpagam University, Coimbatore,
Tamilnadu, India.

Abstract: **Cloud computing is a way to increase the capacity or add abilities dynamically without advancing in brand new infrastructure, training fresh workers, or allowing new software. It spreads information technology's (IT) existing abilities. In the last few years, cloud computing has grown from being a talented business concept to one of the fast-growing sectors of the IT sectors. Despite all the hype surrounding the cloud, initiative regulars are still unwilling to deploy their business in the cloud. Security is one of the foremost issues that reduced the growth of cloud computing and problems with data privacy, and data security remained to an outbreak the market. A new model aiming at improving features of a surviving model must not risk or threaten and vulnerability's other important features of the current model. In this paper, a review of the dissimilar security risks that pose a threat to the cloud is made in.**

Keywords: Cloud Security, Privacy Control, Threat, Vulnerabilities Data Control, Encryption, Data Privacy, confidentiality.

I. INTRODUCTION

Cloud security, the recent rash of visible breaches at high-profile establishments as aim, Anthem, and others, and the subsequent loss each cause, concerns are climbing to make sure their cloud computing, regardless of whether on private, public, or hybrid clouds, are harmless. However, cloud security is multipath. Through transient applications and services, lively up around multiple data centres, with dozens or hundreds of free micro services, each with their own access mechanisms, with the widespread acceptance of virtualization and the recent extensive rage over containerization, care on top of cloud-specific security vulnerabilities are a huge effort in itself.

A. *Characteristics of cloud computing.*

The cloud model helps availability and is collected of five essential characteristics, four service models, and four deployment models.

The salient characteristics of cloud computing are based on the definitions provided by the National Institute of Standards and Terminology (NIST). Here are five characteristics (i) On-demand self-service (ii) Broad network access (iii) Resource pooling (iv) Rapid elasticity (v) Measured service. On-demand self-service: A consumer can unilaterally provision computing abilities, such as associated time and network storage, as needed robotically deprived of requiring human interaction with each provision's provider. A broad network access: Skills are available to the network and accessed through standard mechanisms that promote the use by heterogeneous thin or thick client platforms. Resource pooling: The provider's cloud computing resources are pooled to serve multiple clients using a multi-tenant model, with altered physical and virtual funds dynamically assigned and reassigned according to consumer demand. In the foreground is a sense of location-independence in that the customer usually has no control or knowledge over the exact location of the provided resources, but may be able to specify a location at a higher level concept (e.g., Country, statement, or datacenter). Examples of positions include storage, control, memory, network bandwidth, and virtual machine.[1]

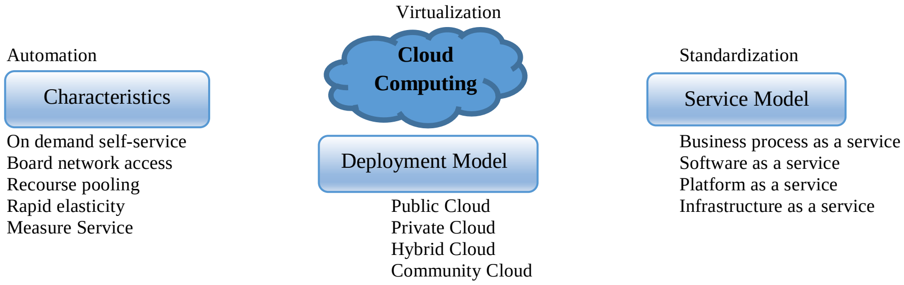

Fig-1 The cloud model promotes availability and is composed of five essential characteristics, four service models, and four deployment models.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

Rapid elasticity: Capabilities can be quickly and elastically provisioned, in some cases, mechanically, too fast scale out and fast released to hurriedly scale in. To the consumer, the abilities available for provisioning often appear to be unlimited and can be purchased in any expanse at any time. Stately service: Cloud systems automatically control and optimize resource use by leveraging. [2]

Metering capability at some level of abstraction appropriate to the type of service (e.g., Storage, dispensation, bandwidth, and lively user accounts). Resource usage can be succeeded, controlled, and reported providing slide for both the provider and consumer of the utilized service. [7]

B. *Deployment model*

A cloud deployment model can be deployed using any of the below mentioned. Here stand four models include 1) Private cloud 2) Public cloud 3) Hybrid cloud 4) Community cloud. Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., Business units). It may be owned, managed, and operated by the group, a third party, or some blend of them, and it may exist on or off buildings. Public cloud: The cloud infrastructure is provisioned for open use by the overall public. It may be possessed, managed, and operated by a business, hypothetical, or government, foundation, or some combination of them. It exists on the premises of the cloud provider. Hybrid cloud: The cloud structure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique units, but are bound together through standardized or exclusive technology that enables data and application portability (e.g., Cloudburst for load balancing between clouds). Community Community cloud: The cloud infrastructure is provisioned for exclusive use of a specific community of consumers from organizations that have collective fears (e.g., Assignment, security requirements, policy, and compliance reflections). It may be owned, managed, and operated by one or more of the organizations in the public, a third party, or some blend of them, and it may be on or off places. [4]

C. *Service model*

There are three mostly service models include-(myself) Software as a Service (SaaS) (ii) Platform as a Service (PaaS) (iii) Infrastructure as a Service (IaaS). Software as a Service (SaaS): Customers obtain the facility to access and use an application or service that is hosted in the cloud. For example 'Salesforce.com', where needed information about the interaction between the consumer, and the service is hosted as part of the service in the cloud. Platform as a Service (PaaS): Customers obtain access to the platforms by enabling them to organize their own software and applications in the cloud. Infrastructure as a Service (IaaS): The facility provided to the customer is to lease processing, storage, and other fundamental computing possessions. The customer does not accomplish or control the basic cloud infrastructure but has control over operating systems, storage, organizer applications. [8]

II. LITERATURE REVIEW

Used Amin Soofi et al (2014) in his paper "Encryption Techniques for Cloud Data Confidentiality "[2] has reviewed the encryption techniques used for the data confidential. The suggestions of review are classified on the basis of type of approach, and the type of validation used to validate the approach.

K. S. Preeti et al (2014) in her work "Implementation of Private Cloud Computing Using Integration of JavaScript and Python"[3] has integration of two prevalent language's JavaScript and python, which is provided with a new level of compliance, which helps in developing an understanding between Web Programming and Application Programming.

Deepika Saxena et al (2014) in his paper "A REVIEW ON DYNAMIC FAIR PRIORITY TASK SCHEDULING ALGORITHM IN CLOUD COMPUTING"[4] provided a review on different task scheduling algorithms and made a review on a proposed task scheduling algorithm named "Dynamic right priority task scheduling algorithm" in cloud computing.

Mayanka Katyal et al (2014) in her paper" Application of Selective Algorithm for Effective Resource Provisioning in Cloud Computing Environment"[5] discusses a selective algorithm for allocation of cloud resources to the end-users on-demand basis. This algorithm is based on minimum-minimum and max-minimum algorithms. These are two conventional task scheduling algorithm. The selection algorithm uses certain heuristics to select between the two algorithms so that overall makes span of the tasks on the machines is minimized.

Tejinder Sharma et al (2013) in his paper "Efficient and Enhanced Algorithm in Cloud Computing"[6] proposes an efficient and enhanced scheduling algorithm that can maintain the load balancing and provides better improved strategies through efficient job scheduling and modified resource allocation techniques. Load balancing ensures that all the processors in the system as well as in the network did approximately the equal amount of work at any instant of time.

III. SECURITY ISSUES IN CLOUD COMPUTING

Security in the cloud is realized, in part, through a third party the controls and assurance much like in traditional outsourcing measures. However, since there is no common cloud computing security standard there are additional challenges associated. Many cloud vendors appliance their individual copyrighted standards and cloud security technologies, and implement differing from cloud security models, which need to be appraised on their individual merits. In a vendor cloud model, it is ultimately down to adopting customer organizations to ensure that

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

security in the cloud meets their own security policies through requirement gathering. Provides risk charges, due diligence, and word activities. Thus, the security challenges faced by organizations wishing to use cloud services are not radically different from those dependents on their own in a house achieved enterprises. The same centre and outside threats are present and require risk mitigation or risk acceptance. This section examines the information security challenges that adopting organization will need to consider. Through declaration activities the vendor or public cloud provider or directly, through designing and implementing security controls in a privately owned cloud.

Cloud brings many different security issues and among them, data security acts as one of the major challenges in cloud computing. Data security and data control becomes an important issue for securing outsourced data and to The table below summarizes the security risks relevant in the cloud:

maintain a level of trust among data owners. In this paper, we will analyse the security requirements and the various approaches for data security. Here also highlight the new emerging research challenges in data security and privacy. [9]

A. *Security risks*

The security risks associated with each cloud delivery model vary and are dependent on a wide range of factors, including the sensitivity of information properties, cloud architectures and security controls involved in a particular cloud locality. The following sections discuss these risks in a general context, except where a specific reference to the cloud delivery model is made.

Risk	Description
Privileged user access	Cloud providers generally have unlimited access to user data, controls are needed to address the risk of privileged user Access leading to compromised customer data.
Data location and segregation	Customers may not distinguish where their data is being stored and there may be a risk of data being stored alongside other customers' information.
Data disposal	Cloud data deletion and disposal are at risk, mostly where hardware is dynamically issued to customers based on their Needs. The risk of data not actually deleted from data stores, Backups and physical media during take out are enhanced within the cloud.

Table 1 - Cloud security risk

IV. SECURITY ALGORITHM USED IN CLOUD COMPUTING.

Data confidentiality and audit ability, topped the list of primary obstacles for the use of cloud computing technologies in their administrations, rendering to a recent survey of doing several Indian Business Technology professionals. Data Security is Top Adoption Obstacle to Cloud in India The survey, conducted by Saltmarch Intelligence in the third quarter of this year measured perceptions of Business technology professionals, including their important challenges in adopting cloud, the drivers, how their organization's plan to use the cloud, the different stages of adoption, and the cloud platforms, applications, clients, infrastructure and storage used. Financial savings, agility and elasticity, all enabled through cloud technology, are crucial in a fast-paced business world.

A. *RSA ALGORITHM*

RSA is basically an uneven encryption, decryption algorithm. It is asymmetric in the sense, that here public key distributed to all through which one can encrypt the message and private key which are used for decryption are kept secret and are not shared to everyone's algorithm is used to ensure the security of data in cloud computing. In RSA algorithm, data is encrypted to provide security. After encryption, the data is stored in the cloud it can be projected, so that when it is required, then a request can be placed to the cloud provider. The cloud provider authenticates the user and delivers the data to a user. As RSA is a Block Cipher in which every message is mapped to an integer.

B. *AES ALGORITHM*

Advanced Encryption Standard (AES), also known as Rijindael is used for securing information. AES is a symmetric block cipher that has been analyzed lengthily and is used widely now-a-days. AES, symmetric key encryption algorithm is used with key length of 128-bits for this purpose. As AES is used widely now-a-days for security of cloud. The implementation proposal states that First, User chooses to use cloud services and will migrate his data on the cloud. Next User submits his service's requirements with Cloud Service Provider (CSP) and chooses best specified services offered by the provider. Whenever an application uploads any data on the cloud, the data will first encrypted using AES algorithm and subsequently sent to the provider. Once encrypted, the data is uploaded to the cloud, any request to read the data will occur after it is decrypted on the users end and then plain text data can be read by the user. The plain text data are never written anywhere on a cloud. This embraces all types of data. This encryption solution is transparent to the application and can be integrated quickly and easily

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

without any changes to the application. The key is never stored next to the encrypted data, since it may compromise the key also. To store the keys, a physical key management server can be installed in the user's premises. This encryption protects data and keys and guarantees that they remain under user's control and will never be exposed in storage or in transit. AES has replaced the DES as approved standard for a wide range of applications.

C. DES ALGORITHM.

The Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of size 64 bits each. Those are 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length of this algorithm is 56 bits; however, a 64 bits key is actually input. DES is, therefore, a symmetric key algorithm [14].

D. BLOWFISH ALGORITHM

Blowfish is a symmetric key cryptographic algorithm. Blowfish encrypts 64 byte blocks with a variable length key of 128-448 bits. According to Schneier, Blowfish was designed with the following objectives in mind:

a. Fast- Blowfish encryption rate of 32-bit microprocessors are 26 clock cycles per byte.
b. Compact- Blowfish can execute in less than 5 KB memory.
c. Simple-Blowfish uses only primitive operation -s, such as addition, XOR and table look up, making its design and implementation simple.
d. Secure- Blowfish has a variable key length up to a maximum of 448-bit length, making it both secure and flexible.

Blowfish suit's applications where the key remains constant for a long time (e.g. Communications link encryption), but not anywhere the key changes frequently.[9]

TABLE 2
Merits and Demerits of Security Algorithms

Methods	Merits	Demerits
RSA ALGORITHM	The purpose of securing data is that only concerned and authorized users can access it	There are many secret-key encryption methods that are significantly faster than currently available public-key encryption method.
Data Encryption Standard (DES)	It was the first encryption standard; DES is 64 bits key size with 64 bit block size.	It uses one private key for encryption as well as for decrypts, So if we lost that key to decrypt the data, then we cannot get the readable data at the receiving end.
Advanced Encryption Standard (AES)	It encrypts data blocks AES is an important advance and using and understanding it will greatly increase the reliability and safety of data security teams.	It has a fixed block size of 128 bits and key size of 128, 192 and 256 bits. If the key size is 128 bits, AES performed 10 rounds, if the key size is 192 bits, it performs 12 rounds and if the key size is 256 rounds, it performs 14 rounds.
BLOWFISH ALGORITHM	It is one of the most common public algorithms; Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful in this, Blowfish algorithm over other algorithms in terms of the processing time.	The disadvantages of Blowfish are it must get the key to the person out of the band, specifically not through the unsecured transmission channel. Each pair of users' needs a unique, so as the number of users increase, key management becomes complicated.

V. CONCLUSION

This study suggests an introduction of cloud computing with the importance of data confidentiality in this field. A literature review of the works regarding to usage of encryption techniques in the area of cloud computing, data security is conducted and the results of the review are presented. This paper produces a baseline security analysis of the cloud computing operational Environment in terms of threats, vulnerabilities and effects.

REFERENCES

[01]. "NIST Cloud Computing Definition," NIST SP 800- 145]

[02]. Aized Amin Soofi, M.Irfan Khan and Fazal-e-Amin "Encryption Techniques for Cloud Data Confidentiality"- International Journal of Grid Distribution Computing Vol.7, No.4 (2014),

[03]. K.S.Preeti,Vijit Singh, Manu Sheel Gupta "Implementation of Private Cloud Computing Using Integration of JavaScript and Python"- The Python Papers Monograph 2: 19 Proceedings of PyCon Asia-Pacific 2010

[04]. Deepika Saxena, Dr. R.K. Chauhan "A REVIEW ON DYNAMIC FAIR PRIORITY TASK SCHEDULING ALGORITHM IN CLOUD COMPUTING"- International Journal of Science, Environment ISSN 2278-3687 (O) and Technology, Vol. 3, No 3, 2014

[05]. Mayanka Katyal , Atul Mishra" Application of Selective Algorithm for Effective Resource Provisioning In Cloud Computing Environment"- International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol. 4, No. 1, February 2014

[06]. Tejinder Sharma,Vijay Kumar Banga "Efficient and Enhanced Algorithm in Cloud Computing"-International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013.

[07]. Weiwei Lina, James Z. Wangb, Chen Liangc and Deyu Qia, "A Threshold-based Dynamic Resource Allocation Scheme for Cloud Computing", 2011, 1877-7058, Elsevier Ltd, PEEA 2011 Doi:10.1016/j.proeng.2011.11.2568, page no: 695 – 703.

[08]. Vijindra and Sudhir Shenai. A, "Survey of Scheduling Issues in Cloud Computing", 2012, ICMOC-2012, 1877-7058, Elsevier Ltd, Doi: 10.1016/j.proeng.2012.06.337, page no: 2881 – 2888.

[09]. Secure User Data in Cloud Computing Using Encryption Algorithms-International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926 1922 | P a g e

[10]. Evaluation of DES, TDES, AES, Blowfish and Two fish Encryption Algorithm: Based on Space Complexity- International Journal of Engineering Research & Technology (IJERT)-ISSN-2278-0181- Vol. 3 Issue 4, April – 2014.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)