A Review of Data Security Issues in Cloud Environment

Sahil Zatakiya
Department of Computer Science & Engineering
B.H.Gardi College of Engineering, Rajkot
Gujarat, India

Pranav Tank
Department of Computer Science & Engineering
B.H.Gardi College of Engineering, Rajkot
Gujarat, India

ABSTRACT
Cloud computing technology is becoming as the next generation architecture of IT industry. It offered many services over the internet. So it is novel pattern of computing where resources are provided on demand via internet. Being pay-as-you-go model, cloud users lease the required resource and pay for their usages only. Today cloud computing is an attractive topic in field of Research and Development. It has many potential advantage and many enterprise applications and data are moving to public or hybrid cloud. But yet many numbers of business-critical applications, organizations, large enterprise wouldn't move them to cloud because of security issues. So from the users' perspective, cloud security concerns, data security and privacy protection issues, remain them primary problem for using cloud computing. In this paper we analyzed security and privacy issues associated with cloud computing and describes some reason for why all IT company are not used cloud and give solution of some issues. Also discuss various attacks against Cloud architecture.

Keywords
Cloud computing, security, Data integrity and privacy.

1. INTRODUCTION
Cloud computing is a new style of Data processing in which client are allowed to use variety of IT services to large poll of computer resources and using the internet as a computation bus. Resources in cloud is looked that can be extended unlimitedly, got 24*7 hours, used on demand and paid according to use. This facility is called using IT service as electricity or water. It is a distributed computing, parallel computing and grid computing development. So The National Institute of Standards and Technology says there are five key features of cloud computing [2]:

- On-demand self-service
- Location-independent resource pooling
- Ubiquitous network access
- Rapid elasticity
- Measured service

This new technology provides mainly three types of services model which can be described "X as a Service (XaaS)" in that X could be infrastructure, platform, or software.

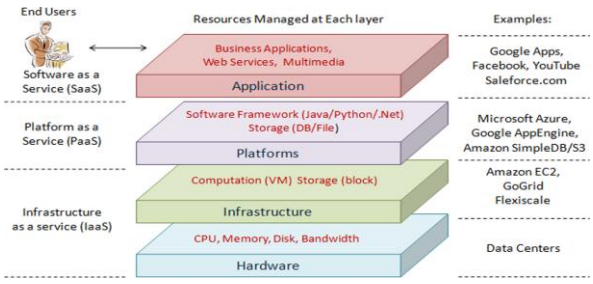

Fig: Cloud Service Model [5]

IaaS is delivery of computer infrastructure such as server, storage, networking technology, and data center spaces as a services. GoGrid, Rackspace Cloud, Amazon are example of IaaS.

PaaS delivers more than IaaS; it is set of software that provides everything to developers needs for the build and run the application. Microsoft Azure, Google's Google apps engine, Salesforce etc. are PaaS providers.

SaaS provides application or software hosted by cloud service provider. Netsuite, Taleo, RightNow, CRM etc. are SaaS providers.

There are three deployment models for cloud computing: Public, Private, and Hybrid [3].

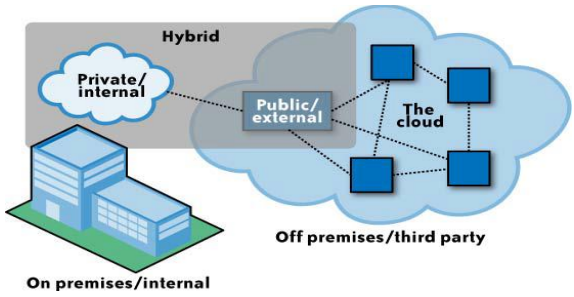

Fig: Cloud Deployment Model [6]

Public cloud: The infrastructure of computing is owned and managed by CSP. Public cloud is used by anyone.

Private cloud: It is highly virtualized cloud data center located inside company's firewall. It may also be a private space dedicated to company within a cloud vendor data center designed to handle company's workload. Your business is part of an industry that must conform to strict security and data privacy issues. A private cloud will meet those requirements.

Hybrid cloud: This model of cloud computing is a composition of two cloud (public or private). Company likes a SaaS application and wants to use it as a standard throughout the company; they concerned about security. To solve this problem, SaaS vendor creates a private cloud just for the company inside their firewall. They provide company with a virtual private network (VPN) for additional security. Now you have both public and private cloud ingredients.

2. SECURITY PROBLEM IN CLOUD
In each field of computer there is big problem with security. If cloud computing is so great, why isn't everyone using it? Today cloud architectures act like big black boxes because after putting data on cloud server user don't know what happen with our data. Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks.

The common security issues in cloud computing across four main categories:

i. Lack of Control: Users' data are store at cloud server. It is only remotely available to users so control over data is some of less rather than personal computer.

ii. Lack of Trust: This category deals with data integrity, data lock in, data confidentiality and user privacy specific concerns.

iii. Access: This comprises the concern around cloud authentication, authorization and access control, encrypted data transfer, and user identity management.

iv. Compliance: Because of its size and disruptive influence, the cloud is attracting attention from regulatory agencies, especially around security audit, data location; operation trace-ability and compliance concerns.

Why every IT industry doesn't move towards cloud computing? There are some reasons of it. And also these are the research problems and issues in cloud environment [15]. Now based on above issues we see security concerns and possible attacks on cloud see in next section.

C1: Co-tenancy in clouds creates new attack vectors: A cloud is shared by multiple users. Malicious users can now legally be in the same infrastructure. Misusing co-tenancy, attackers can launch side channel attacks on victims.

C2: Clients have no idea of or control over what is happening inside the cloud. Clients are forced to trust cloud providers completely.

C3: Clouds provide no guarantee about outsourced data: Dishonest cloud providers can throw data away or lose data. Malicious intruders can delete or tamper with data. A client need reassurance that the outsourced data is available, has not been tampered with, and remains confidential.

C4: Ensuring confidentiality of data in outsourced computation is difficult: Most type of computations require decrypting data before any computations. If the cloud provider is not trusted, this may result in breach of confidentiality.

C5: Privacy is often the victim when using a cloud: It is almost impossible to provide privacy of sensitive personal information in computation outsourcing. Popular distributed computation systems such as MapReduce are not designed with privacy in mind.

C6: Clients have no way of verifying computations outsourced to a Cloud: User sends her data processing job to the cloud. Clouds provide dataflow operation as a service (e.g., MapReduce, Hadoop etc.) Problem is there Users have no way of evaluating the correctness of results.

C7: Assessing the Capability of a Cloud Provider is difficult due to the black box model: Availability, fault-tolerance, and resilience are important to clients for mission-critical data. But cloud providers do not want to reveal their capability or redundancy. So, clients need a way to remotely verify the capability claims.

C8: Data Forensics in Clouds is difficult: Certain Government regulations mandate the ability to audit and run forensic analysis on critical business or healthcare data. Clouds complicate forensic analysis, since the same storage infrastructure is shared by many clients. Cloud providers are not willing to open up their entire storage for forensic investigations.

C9: Clouds can be used for malicious purposes: Adversaries can rent clouds. Temporarily to create a large scale botnet very quickly. Clouds can be used for spamming, Denial of service, brute force password breaking, and other attacks.

C10: Economy matters: Sometimes, economic targets are more effective than technical targets. Attacks can target economic viability of cloud users (by consuming extra resources), or of cloud providers (by fraudulently consuming cloud resources)

3. VARIOUS SECURITY ATTACKS

There is various type of attacks possible in cloud architecture [7]

***A. Denial of Service (DoS) Attacks*:** Cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging. When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power to control additional workload. Thus, the server hardware has maximum workload to process. It is most possible to damage on a service's availability. Thus, the attacker does not have to flood all *n* servers that provide a certain service in target, but only can flood a single, Cloud-based address in order to perform a full loss of availability on the service.

***B. Cloud Malware Injection Attack*:** This attack is the first considerable attack attempt aims at injecting a malicious service implementation or virtual machine into the Cloud system. This attack requires the intruder to create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the intruder has to trick the Cloud system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the intruder. The main idea of the Cloud Malware Injection attack is that an attacker uploads a manipulated copy of a victim's service instance so that some service requests to the victim service are processed within that malicious instance. In order to achieve this, the attacker has to gain control over the victim's data in the cloud system .The attacker controlling the cloud exploits its privileged access capabilities to the service instances in order to attack that service instance's security domains.

***C. Side Channel Attacks*:** An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic algorithms. Evaluating a cryptographic system's resilience to side-channel attacks is therefore important for secure system design.

***D. Authentication Attacks*:** Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example,

based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers. Currently, regarding the architecture of SaaS, IaaS, and Paas, there is only IaaS offering this kind of information protection and data encryption. If the transmitted data is categorized to high confidential for any enterprise, the cloud computing service based on IaaS architecture will be the most suitable solution for secure data communication. In addition, the authorization of data process or management for those data belonged to the enterprises but stored on the service provider's side must be authorized by the user side to instead of the service providers.

***E. Man-In-The-Middle Cryptographic Attacks*:** This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

F. Wrapping Attack Problem: When a user makes a request from his VM through the browser, the request is first directed to the web server. In this server, a SOAP message is generated. This message contains the structural information that will be exchanged between the browser and server during the message passing. Before message passing occurs, the XML document needs to be signed and canonicalization has to be done. Also, the signature values should be appended with the document. Finally, the SOAP header should contain all the necessary information for the destination after computation is done. For a wrapping attack, the adversary does its deception during the translation of the SOAP message in the TLS (Transport Layer Service) layer. The body of the message is duplicated and sent to the server as a legitimate user. The server checks the authentication by the Signature Value (which is also duplicated) and integrity checking for the message is done. As a result, the adversary is able to intrude in the cloud and can run malicious code to interrupt the usual functioning of the cloud servers.

***G. Flooding Attack Problem*:** In a cloud system, all the computational servers work in a service specific manner, with internal communication between them. Whenever a server is overloaded or has reached the threshold limit, it transfers some of its jobs to a nearest and similar service-specific server to offload itself. This sharing approach makes the cloud more efficient and faster executing requests. When an adversary has achieved the authorization to make a request to the cloud, then he/she can easily create bogus data and pose these requests to the cloud server. When processing these requests, the server first checks the authenticity of the requested jobs. Because non-legitimate requests must be checked to determine their authenticity, checking consumes CPU utilization, memory and engages the IaaS to a great extent. While processing these requests, legitimate services can starve, and as a result the server will offload its services to another server. Again, the same thing will occur and the adversary is successful in engaging the whole cloud system just by interrupting the usual processing of one server, in essence flooding the system.

4. SOLUTIONS OF SOME ISSUES

For achieving authentication, data security and verification, at the same time CSP have to use more than one cryptographic algorithm. Example use Digital signature with Diffie Hellman key exchange and AES encryption algorithm [8] and another mechanism is use Digital signature with RSA encryption algorithm [9]. These are the good solution for C3 and C5. For ensuring integrity straightforward encryption mechanism is used. Example HMAC, MD4, MD5, SHA-1, SHA-2 etc [13][12]. For small data file MAC can be used for protect the data integrity and hase tree used for large data file [17]. For the data verification CSP also use Publicly Auditable Secure services mechanism [10]. Integrity and confidentiality of data stored in cloud can either be secured through sealed storage or by making authenticity checks when accessing data. Checksums are useful mechanisms for this. However, checksums are costly to compute and can only be used after transmission of full data to the client (costly for network). New techniques such as Provable Data Possession (PDP) in untrusted cloud may be a more efficient mechanism as it generates a probabilistic proof for data integrity based on only a small portion of the file [18]. If users' data are very sensitive than CSP have to use complex encryption algorithm (example Blowfish, AES, DES with variant key size etc) [11]. The key management can be done through common PKI infrastructure. For solution of C4 New form of encryption, called Homomorphic Encryption is used [16]. It enables the ciphertext to be processed in public cloud without decrypting this. For satisfied C7, proper access control and identity management The Cloud Security Alliance [1] recommends cloud provider to provide stronger authentication mechanism and also (optionally) allow users to use third party identity management and single sign on platforms like Microsoft Passport. This may lead to an added set of authentication complexity. Cloud computing security gateway is to use a new technology[4], the gateway not only to hide sensitive data, can also be the introduction of cloud computing applications within the enterprise, so the companies can either use the services provided by cloud computing, nor Spread out the sensitive corporate data. If it find the sensitive data trying to spread out to an external through the cloud network security gateway, it will be deleted or modified, it also introduces and perform the cloud computing service into the sandbox that the sandbox will prevents any unauthorized access, and it will tells the other users of these sensitive data through tracking cloud data traffic log files. As the key management can control user how to access the protected resources, so it is a core mechanism for the protection of cloud computing data security [4]. Key management system can ensure the key properly that cloud computing can be certified. Therefore, the user must establish a more rigorous key management system to effectively protect the safety of the system that the keys did not go wrong in the generation, distribution, verification, and update, and storage, backup and other sectors. Combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving in public cloud [10]. For C9 One another kind of gateway is Border Gateway Protocol (BGP) architecture is created. The use of this approach should be accompanied by additional protection techniques since it is itself vulnerable to DoS attacks [14]. In [19] Deal with key exchange between cloud user's using cellular automata. It is hard to trace the key by man-in-the-middle-attack because of Strong encryption algorithm (Triple-DES) with CA (Cellular Automata) Rules. Besides CRC (Cyclic Redundancy Check) is done to ensure data integrity at the user's end. Multi-cloud information processing activities (C1) like distributed data mining would require sophisticated privacy preserving models. For C2 and C8, Cloud Security Alliance has created a cloud Governance, Risk Management and Compliance (GRC) toolkit, supported by checklists and questionnaire, for cloud migration audit [1]. For compliance US Federal and other international laws such as the Electronic Communication Privacy Act (ECPA) can

govern concerns for data privacy in cloud [15]. Security Control Automation Protocol (SCAP), promoted by NIST [2], should be a good choice for organizing, expressing, and measuring security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities. For confidential business data CSP can use standard set of data interface and transformation logic. Strong Network Industry Association (SNIA) has suggested a set of mechanism for data remanence problem. All these are possible solution for above concern.

5. CONCLUSION

Cloud Computing emerged as commercial infrastructure paradigm to provide services over the Internet in easy and efficient way. The main reason for possible success of cloud computing is it providing broad category of services through internet to organizations in all over the world. The cloud computing is making the utility computing into a reality. But up to now there are many challenges to be face by the researchers for making cloud computing work well in reality. To protect the data from unauthorized users and to ensure of data security are must required. Security in cloud computing is very much needed as data in the cloud storage are not secure and require lots of attention of user. Some of the challenges like security issues and Data issues are very much required for the users to use the services provided by the cloud. Similarly challenges like Security, performance issues. In this paper we have define the challenges in terms of security issues, data challenges, we also give solution of some problems. We include various attacks with its properties. So For protecting data in cloud we have to develop new mechanisms which provide strong security as well ensuring safety of data and consuming performance cost is less.

6. REFERENCE

[1] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V3.1,http://www.cloudsecurityalliance.org/guidance/csaguide.v3.1.pdf. Nov 2011.

[2] W. Jansen, T. Grance "Guidelines on Security and Privacy in Public Cloud Computing" NIST Special Publication 800-144, December 2011.

[3] Kaufman, Halper , Hurwitz, Bllor "Cloud Computing for Dummies" Wiley India.

[4] RAN Shuanglin "Data Security Policy In The Cloud Computing" IEEE July 14-17, 2012.

[5] Qi Zhang, Lu Cheng, Raouf Boutaba "Cloud computing: state-of-the-art and research challenges" Springer, 20 April 2010.

[6] Tim Mather, Subra, Kumaraswamy, Shahed Latif "Cloud Security and Privacy" O'Reilly, September 2009.

[7] B.Meena, K. Abhishek Challa "Cloud Computing Security Issues with Possible Solutions" International Journal of Computer Science And Technology, Vol. 3, Issue 1, Jan. – March 2012.

[8] Prashant Rewagad, Yogita Pawar "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing" IEEE ,2013.

[9] Uma Somani, Kanika Lakhani, Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" IEEE, 2010.

[10] C. Wang, K. Ren, W. Lou, J. Li "Toward Publicly Auditable Secure Cloud Data Storage Services" IEEE Network , July/August 2010.

[11] Hiren Patel, Dhiren Patel, Jagdish Chaudhari, Sachin Patel, K. Prajapati "Tradeoffs between Performance and Security of Cryptographic Primitives Used in Storage as a Service for Cloud Computing" ACM, September 2012.

[12] M. Dubal, Mahesh T R, Pinaki A Ghosh "Design of New Security Algorithm Using Hybrid Cryptography Architecture" IEEE, 2011.

[13] R. Shaikh , M. Sasikumar "Trust Framework for Calculating Security Strength of a Cloud Service" IEEE , Oct. 19-20, 2012.

[14] Mohamed Hamdi "Security of Cloud Computing, Storage, and Networking" IEEE, 2012.

[15] S.Sengupta, V.Kaulgud, V.Saujanya Sharma "Cloud Computing Security-Trends and Research Directions" IEEE, 2012.

[16] M.Tebaa, S.EL Hajji, A.EL Ghazi "Homomorphic Encryption method applied to Cloud Computing" IEEE, 2012.

[17] B.Makhija, V.Gupta, I.Rajput "Enhanced Data Security in Cloud Computing with Third Party Auditor" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.

[18] Ateniese, G., Burns, R., and Curtmola, R., Provable Data Possession in Untrusted Stores, Proceedings of the 14th ACM conference on Computer and Communication Security, 2007.

[19] Govinda.K, Sathiyamoorthy.E, Surbhit Agarwal "Secure Key Exchange for Cloud Environment Using Cellular Automata with Triple-DES and Error Detection" International Journal of Engineering and Technology, Vol 5 No 2 Apr-May 2013.