# Trend know the security threats and challenges

Business, Management

Trend of IT iscloud computing and it is the modern computing for business and enterprises. Ithelps the enterprises to start their service without initial investment.

It hasmany advantages for provides as well as users with respect to service delivery. Users are increased to adopt the cloud for their computing services. But, thehardest part of the cloud is security. Are the data are kept safe? It isnecessary to know the security challenges on the data outsourced to cloud. Thispaper presents different challenges with respect to security and also describesthe security solution to control it. Cloud users must know the security threatsand challenges before migrate their data or business to cloud environment.

Keywords:-Cloud; Security; Cryptography; Encryption; Data Outsourcing;

I. INTRODUCTIONCloud computing is a new evolving paradigmto a wide range of users like individuals, businesses and governments toprovide virtual resources such as CPUs, memory, hard drives, bandwidth, platforms, and applications in an on-demand environment. Cloud storage hasbecome a boon to the enterprises, to have an infinite space for their data storage1. Every day, the data is growing at a rapidrate in enterprises. To store data, a large number of processing units, harddrives, network infrastructure and other resources are required. Clusters andgrids 2 distributed systems are used to store huge amount of data byenterprises. However, these distributed systems have increased the resourcesrequirements in data management and task scheduling. Additionally, investment in maintaining datacenters and data management increases the financial overhead.

As a result, enterprises store their incredible abundance of data on cloud to reduce datamanagement cost. In addition, an emerging class of entrepreneurs is takingadvantage of clouds as they might not have enough finance to purchase resourcesor ensure the necessary security for data storage and maintenance. The current cloud computing system mainly consists ofthree service models, Software as a Service (SaaS), which provides onlinesoftware to users and it is controlled by CSPs. Platform as a Service (PaaS), which enables the web application developers to easily host their online webapplication on the cloud platforms and user only control the applicationwhatever they are hosted in the cloud. Infrastructure as a Service (IaaS), provides computing infrastructure in virtualized manner based on the usersdemand 3. The cloud system is deployed in four models, Publiccloud, which is operated and controlled by third party service providers and itis accessed by any internet users. It is more cost effective and adaptable toall levels of IT users but it has some security related issues. Private cloud, which is maintained by individual organization or institution, is lunched fortheir computing needs.

It is more expensive and secured cloud model. Communitycloud is used for specific community of users such as Government, Medical andEducation. Hybrid cloud is theintegration of any two or three clouds for maintaining sensitive andinsensitive data. Cloudhas five essential characteristics which provide unique features to the cloudthan other computing 4. On-Demand Self-Service, It enables users to use cloud computing resources  without human intervention between the usersand the Cloud Service Providers(CSP). Broad Network Access, High-bandwidthcommunication links must be

available to connect to the cloud services. High-bandwidth network communication provides access to a large pool ofcomputing resources.

Location-Independent andResource Pooling, Computing resources are pooledto serve multiple users using a multi-tenant model, with different physical andvirtual resources dynamically assigned and reassigned according to users’demand. Applications require resources. However, these resources can be located anywherein the geographic locations physically and assigned as virtual componentswhenever they are needed. Scalability, it enables new nodes to be added or dropped from the network like physicalservers, with limited modifications to infrastructure set up and software. Cloud architecture can scale horizontally or vertically, according to users’demand.

Measured Service, Users are billedautomatically based on the usage of cloud resources. Cloud systems automatically control and optimize resource usagebyleveraging a metering capability at some level of abstraction appropriate tothe type of service (e. g., storage, processing, bandwidth, and active useraccounts).

The cloud computingarchitecture with these layers and four of its deployment models are shown in Figure 1 5. Fig. 1 Services and Deployment Modelsof cloud As the data is stored on Cloud ServiceProviders’ (CSP) servers, confidentiality, integrity, availability, authentication and access control are the most challenging factors in datasecurity. The three pillars of cloud data security are confidentiality, integrityand availability (CIA) 6.

If these requirements are achieved by any cloud community then it isa highly secured system.  But in reality, achieving the CIA is difficult. To achieve a significant role of cloudcomputing security, it isnecessary to have a security model that supports CIA with theadoption of universal standards.

Cloud enables users to outsource their data in anefficient and also cost effective. But, outsourcing data may open differentsecurity related challenges. II.

DATA OURSOUCINGTraditionally, the Data Owners (DOs) archive their data on their own data centers. But theinvestment on data management is very expensive as their data volume is huge. Data outsourcing offers resources for storing the data and sensitiveinformation online wherein the users can take the benefit of privilege toaccess it remotely, avoiding the burden of the data storage 7. Dataoutsourcing has become an essential arrangement for enterprises for datamanagement which includes planning, analysis and servicing of the network. Enterprises use data outsourcingparadigm to store, monitor and maintain their data.

The enterprises which use the dataoutsourcing, hire the computing resources with the capabilities of scalabilityof expanding the resources with a little up-front IT infrastructure investmentcosts 8. Enterprises exploit external servers or third party serviceproviders’ services for data management. Data outsourcing gives benefits toenterprises by reducing or averting the cost involved in investing expensiveresources like hardware, software, upgrading software and hardware, hiringproficient administrators and other experts. In this modern era, cloud computing has emerged as

afeasible and readily available platform to a wide range of users likeindividuals, businesses and governments to store their sensitive andconfidential data which reduces the investment on new software, hardware andstorage medium. There are various types of cloud storage systems. Some of themstore email messages, some for storing pictures, while others store all typesof data in their data pool.

Most of the enterprises use the cloud for archivingtheir data. When, talk about a cloud service provider, hundreds of servers isinvolved. When a data owner stores data in cloud, it is stored in more than oneserver. The CSP maintains the data with their dedicated structure in order tooffer higher availability. With this attribute of CSP, users can access theirdata at any time from any location. TheDOs of enterprises or startups use the advantage of pay-per-use feature ofcloud. Cloud storage is a key for backup outsourcing of any enterprises orgovernment agencies. Since the backup is on cloud, universal access of data ispossible.

This reduces the capital expenditure on resources. It nullifies the storagemanagement problem of DOs as well as ensuring that users can access data fromany location. Hence cloud storage is more versatile and suitable forwell-established businesses as well as startups. A. Issues Arising In Adoption Of Data Outsourcing TheNational Institute of Standards and Technology 9 pinpoints security, interoperability andportability are the major concerns in adoption of cloud. Furthermore, 10, a survey wasconducted by International Data Corporation (IDC) IT group, to rate the cloudservices and its issues in 2009. From the respondents' rating, it is

clearlystated that the security is the major concern in cloud computing paradigm with87. 5% of the votes.

In 11, authorshave reviewed attribute based security issues in cloud. They addressedconfidentiality, integrity, availability, privacy and accountability attributesand the threats against these attributes in their review. As promising as it is, data outsourcing in cloudcomputing is also facing many security issues 12 including data access, data segregation, authentication, authorization, identity management, policy integration, bugexploitation, recovery, accountability, visibility under virtualization, malicious insiders, management console security, account control, and multi-tenancyissues 1314. Analyzing the current security state of cloud storage, it is essentialto identify countermeasures against threats and vulnerabilities 151617. Researches on solutions to various data security issues includecryptography, public key infrastructure, standardization of APIs, and improvingvirtual machine support and legal support 18. Publicclouds clutch the highest risk of data exposure and so it must be managed withproper caution.

Hence understanding the challenges and security risks in cloudenvironment and developing solutions are essential to the success of thisevolving paradigm 19. Securityof data in cloud is a challenge and is of supreme importance as many flaws andconcerns are yet to be identified. The challengingfactors in data security include confidentiality, integrity, availability, dataaccess, data separation, identity management, backup authentication and accesscontrol 20.  The people involved in service providers canget access to the data stored in their servers. In this scenario, if

theservice providers misuse the data for their gain, then it would be a great lossto the data owners. Moreover the multi-tenancy feature of cloud may lead a dataleakage to the other users of the cloud who use the same cloud to store theirdata. Hence, data confidentiality is the most vital factor to be considered tosecure the data in cloud 21.

To ensure dataconfidentiality, cloud providers, data owners and users should take proactivemeasures. The entities of cloud can be public sources or businesses whichprocess sensitive information. The degree of security varies from user to user. The data from public sources may not require a high degree of security.

On the other hand, businesses handlingsensitive data viz banks, other financial establishments or governments requirea high level of security for their sensitive data on cloud. In this scenario, data owners should maintain adequate security measures on their data andapplications. At the same time, attackers can target weaker entity/entities ofa cloud provider which have lack of security in them. Other entities whichreside in the provider may also be compromised. The multi-tenancy nature ofcloud architecture provides chance for malicious attacks on hundreds of sitesby cybercriminals. When the data isstored and maintained by the data owners at their premises, authentication andauthorization mechanisms are enough to protect the data from unauthorizedaccess 22. Since data incloud computing is placed in the hands of third parties, ensuring the dataconfidentiality both at rest and in transit is of greater importance.

As datais stored in the cloud, the user does not know where it is stored and who allcan access the data. Once data is stored on cloud, data owners are disconnectedfrom their data is the most alarming factor 23. Moreover, the cloud data can betampered by inside attackers and outside attackers 24. Inside attackers are the cloud administrators andother personnel related to cloud service provider.

The multi-tenancy 25 feature of cloud allows more than one user to share the resources tostore their data. Henceforth, other users who have access to the same platformof cloud can be the outside attackers. Naturally, the data owners worry about theconfidentiality of the data, since the cloud data can be tampered by insideattackers or outside attackers.

This phenomenon prevents the cloud adoption byenterprises to store their data. To ensure data confidentiality, the dataowners must provide security for their data before they store data on cloud. Hence, a technique should be incorporated tohave the data stored securely on cloud. The technique used for maintaining dataconfidentiality is cryptography 26. Cryptographyprovides security for data storage and data transmission 27. Variouscryptographic algorithms are proposed to encrypt data before the data isoutsourced, which can make the world of cloud storage more secure, reliable andadmirable in such a diminutive time. III. CRYPTOGRAPHY AND CLOUD SECURITYCryptography is the science that is used for information security, where cryptographers jumble the information in order to hide confidentialinformation from any unauthorized users.

The process is known as cipher orcryptographic system 28. Cryptanalysis is “ breaking the code” 29, a technique to obtain the original messagefrom the encrypted message without having any facts and ideas of encryptionparticulars. Cryptology is the study of cryptography and cryptanalysis fields. Cryptography transforms the original message into an unreadable format so thatany malicious users can not access the information 30. The original, meaningful and readable messageis known as plaintext and the scrambled message which gives no meaning is knownas cipher text in the cryptography field.

The process of converting plaintextinto cipher text is called encryption that occurs at data owner’s side. Thecipher text which cannot be understood by any unauthorized people is stored oncloud. When authorized users attempt to access the data, it would be in anencrypted format in cloud 31.

After they receivedata with their credentials, they will decrypt the data to see the contents ofinformation which happens at the user’s side. The reverse process of convertingciphertext into plaintext is called decryption 32. Cryptographic algorithms are categorized into three forms namely: 1) Symmetric algorithm 2) Asymmetric algorithm 3) Data Integrity algorithm - Hash function 26. Symmetric encryption algorithm also known asconventional cryptography uses a single key known as a secret key forencryption and decryption. Asymmetric encryption algorithm, also known aspublic key cryptography, uses two keys: public key is used for encryptionprocess whereas the private key is used in decryption process.

Data integrityalgorithm is used to find out if there are any changes in the data.

Hashfunction accepts any message as an input and produces fixed size ofoutput.  It breaks the original messageinto a chunk of data and creates a unique fixed length signature called hashvalue by one-way compression function. Since asymmetric encryptionalgorithms are computationally complex algorithms, they take comparativelylonger time for encryption and decryption processes than symmetric encryptionalgorithm. Due to this reason, symmetric algorithm is suitable for cloudstorage 33. There are two types of symmetric key algorithms viz.

stream cipher and blockcipher 34. Stream cipher encrypts one bit at a time whereas block cipher encrypts a fixedlength of data referred as a block of data at a time. Generally, block cipheralgorithms are used for dealing with huge amounts of data whereas stream cipheralgorithms are meant for less computational applications but it can handle onlysmall size of data. Additionally, block ciphers are hardware and softwareoptimized algorithms 35. Since encryption occurs on a group of data at a time with feedback modes, blockciphers are not prone to attacks 36. Due to all theaforementioned factors block cipher symmetric encryption algorithms are wellsuitable to secure cloud data in terms of achieving confidentiality. IV.

SECURITY CHALLENGES ON OUTSOURCED DATA IN CLOUDData in the cloud is in transit or at rest, attacks on data arepossible.  The attacks can be in the formof active attack and passive attack 37. Passive attacks are in thenature of interception attacks which compromises the confidentiality of data. Active

attacks can be in three natures:§ Interruptionattack on availability of data§ Modificationattack on integrity of data § Fabricationattack on authenticity of data. Confidentialityensures only the authorized users can gain access to the data.

Confidentialityguards the data from unauthorized users gaining knowledge of transmittedinformation contents. Thefollowing are some of the vulnerabilities in a cloud 38. Some of the open issues and threats that needs urgent attention are asfollows1. Shared Technology vulnerabilities – increasedleverage of resources gives the attackers a single point of attack, which cancause damage disproportional to its importance. An example of share technologyis a hypervisor or cloud orchestration. 2.

Data Breach – with data protection movingfrom cloud consumer to cloud service provider, the risk of accidental, malicious, and intentional data breach is high. 3. Account of Service traffic hijacking – one of thebiggest advantages of cloud is access through Internet, but the same is a riskof account compromise. Loosing access to privileged account might mean loss ofservice4. Denial of Service (DoS) – any denial ofservice attack on the cloud provider can affect all tenets5. Malicious Insider – a determinedinsider can find more ways to attack and cover the track in a cloud scenario. 6.

Internet Protocol – manyvulnerabilities inherent in IP such as IP spoofing, ARP spoofing, DNS Poisoningare real threats. 7. Injection Vulnerabilities – vulnerabilities such as SQL injection flaw, OS injection, and LDAP injection atthe management layer can cause major issues across multiple cloud

consumers. 8. API & Browser Vulnerabilities – Anyvulnerability in cloud provider’s API or Interface poses a significant risk, when coupled with social engineering or browser based attacks; the damage canbe significant. 9. Changes to Business Model – cloudcomputing can be a significant change to a cloud consumer’s business model.

ITdepartment, and business needs to adapt or face exposure to risk. 10. Abusive use – certain features of cloudcomputing can be used for malicious attack purposes such as the use of trailperiod of use to launch zombie or DDoS attacks.

11. Malicious Insider – a maliciousinsider is always a major risk, however, a malicious insider at the cloudprovider can cause significant damage to multiple consumers. 12. Availability –the probability that a systemwill work as required and when required. V. SECURITY MEASURES AND SOLUTION The vulnerabilities and threats in thecloud are well documented. Each cloud service provider and cloud consumer hasto devise security measures and controls to mitigate the risks based on theirassessment.

However, the following are some of the best practices incountermeasures and controls that can be considered: Ø End-to-endencryption –the data in a cloud delivery model might traverse through many geographicallocations; it is imperative to encrypt the data end-to-end. Ø Scanning formalicious activities – end-to-end encryption while highly recommended, induces new risks, as encrypted data cannot be read by the Firewall or IDS. Therefore, it is important to have appropriate controls and countermeasures tomitigate risks from malicious software passing through encryption.

Ø Validation ofcloud consumer– the cloud provider has to take adequate precautions to screen the cloudconsumer to prevent important features of cloud being used for malicious attackpurposes. Ø SecureInterfaces and APIs – the interfaces and APIs are important toimplement automation, orchestration, and management. The cloud provider has toensure that any vulnerability is mitigated. Ø Insider attacks – cloudproviders should take precaution to screening employee and contractors, alongwith strengthening internal security systems to prevent any insider attacks. Ø Secure leveragedresources– in a shared/multi-tenancy model, the cloud provider has secure sharedresources such as hypervisor, orchestration, and monitoring tools. Ø BusinessContinuity plans –Business continuity plan is a process of documenting the response of the organizationto any incidents that cause unavailability of whole or part of abusiness-critical process. VI.

CONCLUSIONCloud provides huge amount of computingresources. But, it has some security related hurdles to adopt its services. Cloud users must know these security challenges in cloud before start use theservices. This paper presented a detailed view of cloud computing basis and thesecurity challenges.

The paper has also described security threats andsolutions to control security attacks. If all issues related to security areaddressed, then cloud users can use safe cloud environment.