A Survey on Security Issues in Cloud Computing

Stephy Davis
Department of computer science
St. Joseph's college (Autonomous)
Irinjalakuda, Thrissur, Kerala

Ambily Jacob
Department of computer science
St. Joseph's college (Autonomous)
Irinjalakuda, Thrissur, Kerala

***Abstract*—— Cloud computing provide on demand computational infrastructure to the users which has the latent to reduce the huge cost to assemble IT based services. It can offer ubiquitous, expedient data storage space. One of the main significant issue of cloud computing is that the entire data are stored in different location of the world using a set of interconnected resource pools and an authorized user can access this data through virtual machines. Most of the today's internet companies have built immense data centres and day by day it is growing incredibly. For this reason we are getting various types of cloud flavour in terms of excellent applications or services. But it has several dark sides and insecurity creates major problem for cloud users. Since the resource pools are situated over various corners of the world, the privacy and security of data is highly challenging. Due to new dimension of cloud computing, the security problem enters into the problem scope related flexibility, multi-tenancy, layer dependency over its architecture. There are several types of security issues that need to be address in cloud computing. The main aim of this paper is to focus on various security issues of cloud computing and analyse the different unsolved security problem that threatening the different organization to adopt this technology**

Keywords— Cloud computing, Data security, access control, security measures, privacy

I. INTRODUCTION

Cloud computing is rapidly increasing technology and it has changes the software from server to services. Various cloud service providers such as Amazon web services (AWS), Microsoft Azure etc. provide different services to user on (PAYG) pay as you go basis. As per the definition of NIST [2] "Cloud computing is a Internet computing for ubiquitous and on demand access to resources delivered to users" [2]. The user can access any type of resources from anywhere, anytime around the world. Cloud computing uses virtualization technology and utility computing. Cloud computing enables to access the data from anywhere using Internet. Security of data is one of the major issue in cloud computing. Due to centralization of data, the data on the cloud server is more prone to risk and attacks. Security of data is also affected due to multitenant environment. In multitenancy resources are shared among users [1]. This can be also be used for scalable and large level applications. Strong security measures must be employed to handle such challenges.

A. Cloud service models

Cloud computing offers a large variety of services to its users. The users can use these services online and they have to pay for what they use. In this section we will discuss various service models of cloud 1) Infrastructure as a service (IaaS) This layer is at the bottom of the cloud model. IaaS mainly deals with servers, computer, hardware, storage, processor, memory etc. Users can rent any IT infrastructure and he has to pay for that service. The user can rent any server or hardware and pays for it instead of purchasing them. 2) Platform as a service (PaaS) This is at the middleware of service model. This model delivers services in the form providing platform, framework which enables the users to develop and test their software as well as mobile applications. The services of PaaS is more flexible SaaS model services. The security of PaaS can be compromised in the deployment of customer application

B. Cloud Deployment Models

The deployment model tells the nature of cloud. Consistency of data is achieved by resource sharing.

1) Public Cloud It is owned by third party service provider. Public cloud has open access to public and organizations. The user has to pay for the service which he is using. The public cloud may be owned and operated by government organizations

. 2) Private Cloud The private clouds are owned by particular organizations or business. The user of that organization can use the services of cloud. The relationship of customer and CSP can be easily identified because the cloud is owned explicitly by a particular organization

. 3) Hybrid Cloud This cloud contains features of both public and private cloud

II. SECURITY IN CLOUD COMPUTING

- Confidentiality and privacy

Confidentiality refers to solely approved parties or systems having the flexibility to access protected knowledge. The threat of information compromise will increase within the cloud, because of the raised variety of parties, devices and applications concerned, that results in a rise within the variety of points of access. A number of considerations emerge concerning the problems of multitenancy, data remanence, application
security and privacy [3]. Multitenancy refers to the cloud characteristic of resource sharing. Several aspects of the IS square measure shared together with, memory, programs, networks and data. Cloud computing relies on a business model within which resources square measure shared (i.e., multiple users use the same resource) at the network level, host level, and application level. Although users square measure isolated at a virtual level, hardware is not separated. With a multitenant design, a software application is designed

to virtually partition its data and configuration so that each client organization works with a customized virtual application instance. Multitenancy, is relative to multitasking in operating systems. In computing, multitasking is a method by which multiple tasks, also known as processes, share common processing resources such as a CPU. Multitenancy, as multitasking, presents a number of privacy and confidentiality threats. Object reusability is a very important characteristic of cloud infrastructures, but reusable objects must be carefully controlled lest they create a serious vulnerability. Data confidentiality can be breach accidentally, because of knowledge remanence. Data remanence is that the residual illustration of information that are in a way nominally erased or removed. Due to virtual separation of logical drives and lack of hardware separation between multiple users on one infrastructure, knowledge remanence might cause the unwilling revealing of personal knowledge. But also maliciously, a user may claim a large amount of disk space and then hunt for sensitive data. Data confidentiality within the cloud is correlative to user authentication. Protecting a user's account from larceny is AN instance of a bigger downside of dominant access to things, including memory, devices, software etc. Electronic authentication is that the method of building confidence in user identities, electronically conferred to AN system. Lack of sturdy authentication will cause unauthorized access to users account on a cloud, leading to a breach in privacy.

- ***Integrity***

A key aspect of Information Security is integrity. Integrity implies that assets will be changed solely by approved parties. Data Integrity refers to protective knowledge from unauthorized deletion, modification or fabrication. Authorization is that the mechanism by that a system determines what level of access a selected echt user ought to have. Due to the raised variety of entities and access points in an exceedingly cloud atmosphere, authorization is crucial in assuring that only authorized entities can interact with data

- ***Availability***

Availability refers to the property of a system being accessible and usable upon demand by a certified entity. System accessibility includes a systems ability to hold on operations even once some authorities act. The system should have the flexibility to continue operations even within the chance of a security breach. Availability refers to knowledge, software but also hardware being available to authorized users upon demand. The network is burdened with data retrieval and processing. The cloud owner has to guarantee that info and data process is offered to purchasers upon demand. Verifying identities several of that share common basic security necessities, and determining specific needs for data protection and information security

can be one in every of the foremost complicated parts of IS style. This multiuser distributed atmosphere proposes distinctive security challenges, dependent on the level at which the user operates.

The security objectives within a distributed system are essential[8]: • to ensure the availability of information communicated between participating systems; • to maintain the integrity of information communicated between participating systems, i.e. preventing the loss or modification of knowledge because of unauthorized access, component failure or other errors; • to maintain the integrity of the services provided, i.e. confidentiality and correct operation; • to provide control over access to services or their components to ensure that users may only use services for which they are authorized; • to demonstrate the identity of human action parties (peer entities) and wherever necessary (e.g. for banking purposes) to make sure non-repudiation of information origin and delivery; and • wherever applicable, to produce secure interworking with the non-open systems world.

III. DATA STORAGE AND SECURITY IN THE CLOUD

Many cloud service suppliers offer storage as a kind of service. They take information|the info|the information} from the users and store them on massive data centres, thus providing users a method of storage. In spite of claims by the cloud service suppliers concerning the protection of the info keep within the cloud there are cases once the info keep in these clouds are changed or lost because of some security breach or some human error. Attack vectors in a cloud storage platform have been discussed and how the same platform is exploited to hide files with unlimited storage in [4]. In [4], authors have studied the storage mechanism of Dropbox (a file storage solution in the cloud) and carried three types of attack viz. Hash price manipulation attack, stolen host id attack and direct download attack. Once the host id is known, the attacker can upload and link arbitrary files to the victim's Dropbox account.

Various cloud service suppliers adopt totally different technologies to safeguard the info keep in their cloud. But the question is: Is the data stored in these clouds really secure? The virtualized nature of cloud storage makes the standard mechanisms unsuitable for handling the safety problems . These service suppliers use totally different cryptography techniques such as: public key cryptography and personal key cryptography to secure the info keep within the cloud. A similar technique providing data storage security, utilizing the homomorphic token with distributed verification of erasure-coded data has been discussed in [5]. Trust primarily based strategies square measure helpful in establishing relationships in a very distributed setting. A domain based trust-model has been proposed in [6] to handle security and interoperability in cross clouds. Every domain incorporates a agent for trust management. It proposes totally different trust mechanisms for users and repair suppliers.

The following aspects of information security ought to be taken care whereas getting into a cloud:

1. Data-in-transit
2. Data-at-rest
3. Data Lineage
4. Data Remanence
5. Data Provenance

In case of data-in-transit, the biggest risk is associated with the encryption technology that is being used, whether it is up-todate with the present day security threats and makes use of a protocol that has confidentiality similarly as integrity to the data-in-transit. Simply going for Associate in Nursing cryptography technology doesn't serve the aim. In addition to

using an encryption – decryption algorithm for secure data transfer, data can be broken into packets and then transferred through disjoint paths to the receiver. It reduces the chances of all the packets being captured by an adversary. And the information can not be glorious till all the packets square measure coupled along in a very specific manner. A similar approach has been discussed in [7,8].

Managing information at rest in Associate in Nursing IaaS state of affairs is a lot of possible compared to managing constant over a SaaS and PaaS platform as a result of restricted rights over the info. In a SaaS and PaaS platform, data is generally commingled with other users' data. There have been cases wherein even after implementing data tagging to prevent unauthorized access, it was possible to access data through exploitation of application vulnerability . The main issue with data-at-rest in the cloud is loss of control, even a non-authorized user/party may have access to the data (it is not supposed to access) in a shared environment. However, now-a-days, storage devices with in-built encryption techniques are available which are resilient to unauthorized access to certain extent. Even in such a case, nothing can be done in case the encryption and decryption keys are accessible to the malicious user. A lockbox approach wherein the actual keys are stored in a lockbox and there is a separate key to access that lockbox is useful in the above mentioned case. In such a state of affairs, a user will be provided a key based on identity management technique corresponding to the COI (community of interest) he belongs to, to access the lockbox. Whenever the user desires to access the info, he needs to acquire the COI key to the lockbox and then the user gets appropriate access to the relevant data . Homomorphic cryptography techniques, that square measure capable of process the encrypted information so transportation back the info into its original type, also are providing higher means that to secure the data-at-rest. A simple technique for securing data at rest in a cloud computing environment has been mentioned in [9]. This technique makes use of public encryption technique.

Tracing the data path is known as data lineage and it is important for auditing purpose in the cloud. Providing knowledge lineage could be a difficult task during a cloud computing setting and a lot of therefore during a public cloud. Since the data flow is no longer linear in a virtualized environment within the cloud, it complicates the process of mapping the data flow to ensure integrity of the data. Proving knowledge place of origin is one more difficult task during a cloud computing setting. Data provenance refers to maintaining the integrity of the data, ensuring that it is computationally correct. Taxonomy of provenance techniques and various data provenance techniques have been discussed in [10].

Another major issue that's largely neglected is of DataRemanence. It refers to the data left out in case of data transfer or data removal. It causes minimal security threats in private cloud computing offerings, however severe security issues may emerge out in case of public cloud offerings as a result of data-remanence [11,13].

Various cases of cloud security breach came into lightweight in recent past. Cloud primarily based email selling services company, Epsilon, suffered an information breach, because of that an outsized section of its customers as well as JP Morgan Chase, Citibank, Barclays Bank, hotel chains such as Marriott and Hilton, and big retailers such as Best Buy and Walgreens were affected heavily and huge chunk of customer data was exposed to the hackers which includes customer email ids and bank account details [12].

A similar incident happened with Amazon inflicting the disruption of its EC2 services. Popular sites like: Quora, FourSquare and Reditt were the main sufferers [14]. The on top of mentioned events depict the vulnerability of the cloud services.

Another vital facet is that the acknowledged and fashionable domains are wont to launch malicious software system or hack into companies' secure information. A similar issue happened with Amazon's S3 platform and the hackers were able to launch corrupted codes using a trusted domain [15]. Hence the question that arises now could be United Nations agency to be provided the "trusted" tag. It established that Amazon was vulnerable to side-channel attacks, and a malicious virtual machine, occupying the same server as the target, could easily gain access to the confidential data . The question is: ought to any such security policy be in situ for these trustworthy users as well?

An incident related to the data loss occurred, sometime back, with the online storage service provider "Media max" (also known as "The Linkup") when due to system administration error; active customer data was deleted, leading to huge data loss [16]. SLA (Service Level Agreement) with the Cloud Service suppliers ought to contain all the points which will cause knowledge loss either because of some human or system generated error. Hence, it should be ensured that redundant copies of the user knowledge ought to be keep so as to handle any kind of adverse scenario resulting in knowledge loss.

Virtualization normally will increase the protection of a cloud setting. With virtualization, one machine may be divided into several virtual machines, so providing higher knowledge isolation and safety against denial of service attacks . The VMs (Virtual Machine) provide a security test-bed for execution of untested code from un-trusted users. A hierarchical reputation system has been proposed in the paper [17] for managing trust in a cloud environment

IV. MITIGATING SOLUTIONS TO SECURITY AND PRIVACY

After studying the literature, I have identified various methods which can be proposed as better solutions for data security and privacy.

A. Encryption Techniques

The best solution for data security is encryption techniques. Whenever data is stored on the cloud it should be in encrypted format. The encryption techniques can be of any type: symmetric or asymmetric encryption. In symmetric technique shared secret key is used by both sender and receiver to encrypt and decrypt the data. In asymmetric method public and private keys are used for encryption and decryption . The data to be stored on cloud should follow confidentiality, integrity and it should be authentic. In order to prevent access of data by other users it is important to encrypt that data before storing it on the cloud . There should be clear

boundaries at software as a service to segregate data from different users.

B. *Authentication Methods*

Whenever data is uploaded on the cloud it is beneficial to check if the data has a backup on different drives . The hash of the data can be calculated to maintain the integrity of data. For data integrity check RSA can be used to combine RSA signature with identity based encryption.

C. *Key Management*

The key used for encryption is more prone to attacks. If the key gets compromise, then the data stored on the cloud is also lost. Therefore, proper management of key is very important to ensure data security and privacy. Various key management methods can be used to ensure that key should not get compromised. Key distribution methods can also be applied in cloud computing to ensure that only authentic users can access the data.

D. *Secure API's*

By using authentication protocols for security of API the software applications can be developed safely thereby cutting down malicious activities.

E. *Secure SLA*

Service Level Agreement means the legal commitment between user and cloud service provider. Secure SLA ensures the secure agreement between cloud service provider and users using its services.

V.APPLICATIONS OF CLOUD COMPUTING

A. *Cloud in Health Sector*

- **Ubiquity**: The cloud computing is location independent in which the data can be accessed from anywhere and any part of the world.
- **Home monitoring**: In home monitoring the data of measuring devices used in medical field is encrypted and stored on the private cloud.
- **Collaboration**: By storing the personal data of patient in the private cloud with user restriction the security of data can be increased.
- **Risk:** The risk of data loss due to natural disaster is less as the geographical disaster is unlikely to take down IT systems.
- Windows Azure has developed H1N1 Flu Response Center which enable the users to self-assess their disease and get proper advice.
- The application enables the users to share their information regarding disease to other people.

B. *E-governance*

With the help of cloud computing in public sector the conditions for development of e-governance is increased. The e-governance cover the whole country including local administrative units.

C. *Education Sector*

The cloud computing in education sector helps a lot by enabling students to access different online services of cloud. The student can store and retrieve their data from the cloud

VI. CONCLUSION

Although cloud computing is very beneficial to users and it is the new technology in today's era, it still faces many challenges. The cloud computing is dominating the IT market by giving many benefits to organizations and companies. Security of data is identified as one of the important challenges in cloud. In this paper various security issues and its solutions are provided to reduce the risk involved in cloud computing. Moreover, a comparative analysis of various security issues and its countermeasures are also presented. In future proper key management techniques can be used to distribute the key to various cloud users thereby allowing authorized person to access the data. Also encryption techniques can be used for secure data storage and retrieval from the cloud.

REFERENCES

[1] Abdul Muttalib Khan , Dr. Shish Ahmad , Mohd. Haroon, "A Comparative Study of Trends in Security in Cloud Computing", 2015 Fifth International Conference on Communication Systems and Network Technologies, IEEE 2015
[2] NIST defmition of Cloud. NIST 500-292 "NIST Cloud Computing Reference Architecture"
[3] Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010.
[4] Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, Edgar Weippl, "Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space", Proceedings of the 20th USENIX conference on Security, Berkley, USA, 2011.
[5] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", 17th International workshop on Quality of Service,2009, IWQoS, Charleston, SC, USA, pp.19, July 13-15, 2009, ISBN: 978-1-4244-3875-4.
[6] W. Li, L. Ping, X. Pan, "Use trust management module to achieve effective security mechanisms in cloud environment", 2010 International Conference on Electronics and Information Engineering (ICEIE), Volume: 1, pp. V1-14 - V1-19, 2010. DOI: 10.1109/ICEIE.2010.5559829.
[7] R. A. Vasudevan, A. Abraham, S.Sanyal, D.P. Agarwal, "Jigsaw-based secure data transfer over computer networks", Int. Conference on Information Technology: Coding and Computing, pp. 2-6, vol.1, April, 2004.
[8] R. A. Vasudevan, S. Sanyal, "A Novel Multipath Approach to Security in Mobile Ad Hoc Networks (MANETs)", Int. Conference on Computers and Devices for Communication, CODEC'04, Kolkata, India.
[9] Jeff Sedayao, Steven Su, Xiaohao Ma, Minghao Jiang and Kai Miao, "A Simple Technique for Securing Data at Rest", Lecture Notes in Computer Science, pp. 553558, 2009. DOI: 10.1007/978-3-642-10665-1_51
[10] Yogesh L. Simmhan, Beth Plale, Dennis Gannon, "A Survey of Data Provenance Techniques", ACM SIGMOD, vol. 34, issue. 3, Sep, 2005, NY, USA. DOI: 10.1145/1084805.1084812
[11] P. R. Gallagher, "Guide to Understanding Data Remanence in Automated Information Systems", The Rainbow Books, ch3 and ch.4, 1991.
[12] Larry Dignan (Editor in Chief- ZDNet), "Epsilon Data Breach: What's the value of an email address", IT Security Blogs, Tech Republic, April 5, 2011. http://www.techrepublic.com/blog/security/epsilondata-breach-whats-the-value-of-an-email-address/5307
[13] Farzad Sabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology", Int. Journal of Machine Learning and Computing, pp. 39-45, vol. 2, no. 1, February, 2012.
[14] David Goldman, "Why Amazon's Cloud Titanic Went Down", CNNMoney, April, 2011. http://money.cnn.com/2011/04/22/technology/amazon_ec2_cloud_outage/index.htm

[15] Rory Smith (SOC Analyst), "The Use of Legitimate Channels to distribute malicious software to Users", Security Samurai, Aug. 2, 2011. http://www.thesecuritysamurai.com/2011/08/02/theuse-of-legitimate-channels-to-distribute-maliciousoftware-to-users-by-rory-smith-soc-analyst/

[16] Michael Krigsman, "MediaMax/The Linkup: When the Cloud fails", IT Project Failures, News and Blogs, ZDNet, August, 2008. http://www.zdnet.com/blog/projectfailures/mediamaxthe-linkup-when-the-cloud-fails/999

[17] Kulkarni and Y. Hu, "Cloud security with virtualized defence and Reputation-based Trust management", Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695-3929-4