Security Issues in Cloud Computing

Sanchi Kalra
Computer Science Department
Bharati Vidyapeeth's College of Engineering
Delhi, India

Kunal Atal
Computer Science Department
Bharati Vidyapeeth's College of Engineering
Delhi, India

Rachna Jain
Computer Science Department
Bharati Vidyapeeth's College of Engineering
Delhi, India

ABSTRACT
Cloud computing is a framework for providing various computing and storage services on the on-demand basis via the internet. It provides access to a user pool of shared network and storage resources using the server of the service provider without materially acquiring these resources. Hence, it saves managing cost and time for various organizations as well as individual users. Many industries, such as education, banking, healthcare and manufacturing are widely adapting cloud services due to their efficiency, flexibility and reduction of costs. Since, cloud services are universally accessible; it makes accessing data process a lot easier than traditional storage methods. Some popular cloud providers where client data is stored and maintained are Google, Amazon, SalesForce, Microsoft, etc. However, cloud technology is completely internet dependent and hence, faces as many threats as that are existing in the networks such as intranets. These threats can occur in various forms such as traffic hijacking, insecure interface and APIs, malicious insiders, abuse of cloud services, shared technology vulnerabilities, data breaches, perimeter security model broken or unknown risk profile. The primary objective of this paper is to acknowledge the major issues of security and provide a solution to overcome them.

Keywords
Cloud Computing, Data Security, Compression, Encryption, Authenticity, Integrity

1. INTRODUCTION
Cloud computing is the architecture for equipping computing services, such as, servers, software, storage, databases, etc, over the internet. It is very similar to billing of electricity or water as clients are directly debited for the cloud services bank on to their usage. [1]. Cloud computing is basically based on ***dissolution of computing resources*** rather than having provincial servers or exclusive devices to handle different applications. [2]. Cloud uses large group of heterogeneous servers running on low cost clientele PC technologies with dedicated connections to distribute data-access and data-processing tasks among them without any biasness. This preliminary structure consists of mammoth number of systems which are concomitant. The paramount application of cloud technology is to provide data storage and to improve competence of gigantic and immersive online computer applications in a consumer-oriented environment. Many a time, virtual versions of servers, networks or desktops are used to augment the potential of cloud computing. The standards and principles for connecting computer systems and the software needed to exhaust all the possibilities of cloud technologies working efficiently are not thoroughly defined at present time, leaving many companies to define their own cloud computing technologies. Major corporations, such as, Amazon, IBM, Google, Sun, Dell, Cisco, HP, Intel, Novell, and Oracle have invested in cloud computing and offer individuals and businesses a variety of cloud-based solutions. Cloud computing systems offered by companies, like IBM's "Blue Cloud" technologies for example, establish open standards and open source software which associate computers, which consequently, are used to deliver fluent Web 2.0 facilities, such as mash-ups or mobile commerce. [3].

Most Cloud services can be categorized as following:

In **Infrastructure as a Service (IaaS)** end users can rent IT infrastructure such as servers, Virtual Machines (VMs), storage, networks, operating systems from a cloud provider on a pay-per-use basis. It supports high-performance computing and trims down expenses by eliminating the cost of managing an on-site data centre, downsizing disaster recovery costs and waiving the cost of maintaining and upgrading software and hardware equipments .[1]. **Platform as a Service (PaaS)** can provide on-demand environment for developing, testing, delivering and managing software applications. It is mostly designed for developers for smooth and mercurial establishment of web or mobile applications, even without being proficient with elementary groundwork of servers, storage, networks and databases, pivotal for development. Users can access these tools over the internet using APIs, web portals or gateway software. Some common PaaS providers are ***Force.com, AWS Elastic Beanstalk*** and ***Google App Engine.*** With **Software as a Service (SaaS)**, software applications, commonly known as Web Services are forwarded to distant systems that are owned and operated by others. These applications are delivered on demand and most commonly on subscription basis. Cloud providers administer the underlying infrastructure of the applications and conduct maintenance work, like software upgrades and security patching. Users connect to application over the internet, usually with a web browser on their phone, tablet or PC. ***Microsoft Office 365*** is a SaaS application for email services. In **Desktop as a Service (DaaS)**, back-end of a Virtual Desktop Infrastructure (VDI) is handled by the cloud service provider. This service is obtained by the customer on the subscription basis and loud provider regulates functionalities such as data storage, backups, security and upgrades. Consumer's privy data is copied to and from the virtual desktop during logon or logoff and access to this desktop is device, location and network independent.

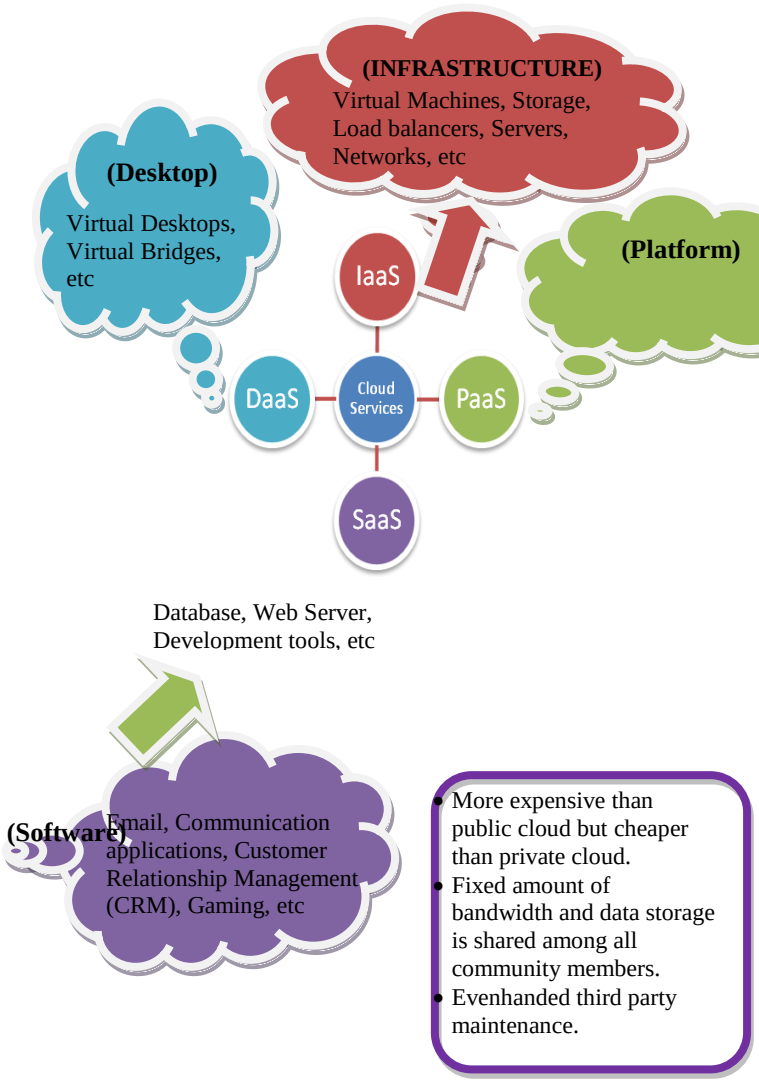

Fig 1: Cloud Computing Services

Cloud Deployment Models are categorized into four types:

Public Cloud can openly be used by general public and a third-party provider delivers the cloud services over the internet. Public cloud services are disposed on demand, by the minute, hour or day. Customers indemnify for the CPU cycles, storage and bandwidth they exhaust. Leading public cloud providers include ***Amazon Web Services (AWS), Microsoft Azure, IBM SoftLayer*** and ***Google Compute Engine.*** **Private Cloud** are used by single organization, including its many employees or business units. It is physically located on the company's onsite data centre. The services and infrastructure are maintained on a private network. **Community Cloud** are used by specific community of customers having their common goals. Several organizations, having the same requirements such as security, privacy, services can share the cloud infrastructure. **Hybrid Cloud** is a combination of two or more above mentioned cloud infrastructures. Hybrid Clouds provides greater flexibility and more deployment options as well as provides better way to take advantage of all the services that these clouds provide independently.

Benefits of Cloud Computing are as follows:

(1) Lower capital expenditure: Cloud computing abolishes the need of a company to invest in storage**,** hardware and servers. Services are accessible on the subscription basis to the clients based on their usage.

(2) 24/7 Support: Since all the services are executed over the internet, a company does not have to worry about technical issues and other problems associated with physical storage and backup. Cloud service providers ensure that all the issues as soon as they occur.

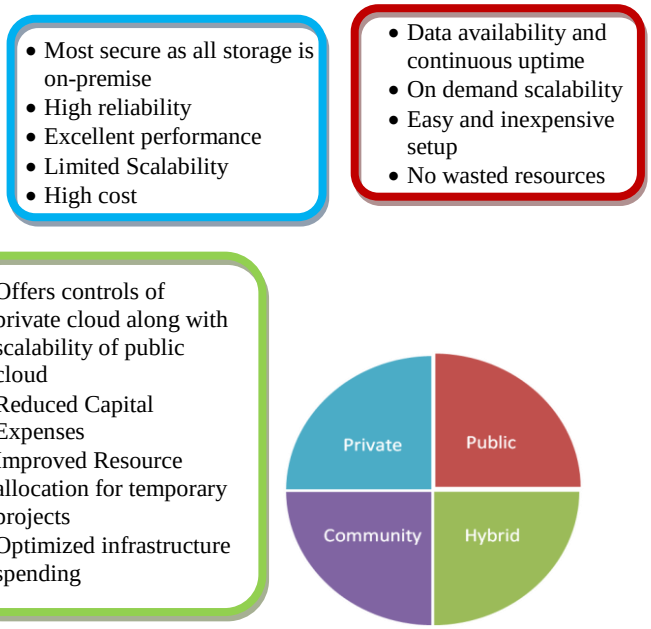

Fig 2: Cloud Computing Deployment Models

(3) Automatic Software Updates: Cloud Service Providers roll out regular software updates which includes updates for security, privacy and privacy. This spares businesses from worrying about maintenance of their software and enables them focus on their core activities.

(4) Easy and Agile Deployment: Cloud computing yields a reliable performance irrespective of the geographical location or the type of device used by the user. It provides users flexibility of working anywhere as the only requirement is of the internet and any device could be used anywhere for the work.

(5) Reliability, Scalability and Sustainability: Cloud Computing offers optimum security which protects users against any unauthorized access, modification and loss of data. Also, cloud can be scaled limitlessly anytime according to the requirements.

(6) Highly automated: Automated services maintain a high level of customer satisfaction. For example: If a part of the cloud environment fails or stops working, there are various troubleshooting processes defined for it. Even if the problem persists, the other resources continue to work until the problem is fixed, so that the work doesn't stop.

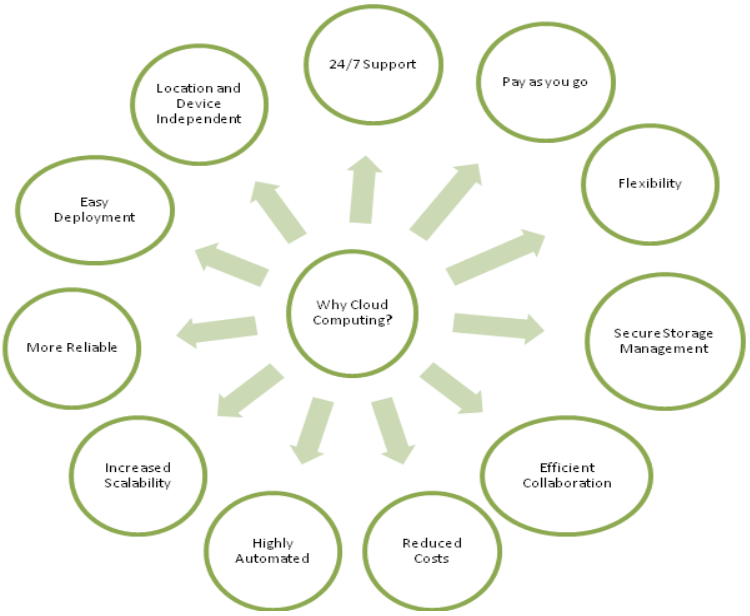

Fig 3: Benefits of Cloud Computing

2. SECURITY ISSUES IN CLOUD COMPUTING

Security is the pre-eminent regard for businesses which yearn to adopt cloud technology, especially public clouds. Public cloud providers disintegrate their underlying hardware infrastructure between legion customers, as public cloud is a multi-tenant environment. This environment demands copious isolation between logical compute resources [5]. Apart from this, cloud technologies suffer from a jillion of threats, such as data breaches, tampering, eavesdropping information disclosure, identity spoofing, viruses and worms, etc [6]. Encryption is the best solution

to prevent security yet not independently sufficient. Thus, there is a need to determine a perfect amalgamation of various security techniques to provide efficient authenticity, integrity and confidentiality to data on cloud.

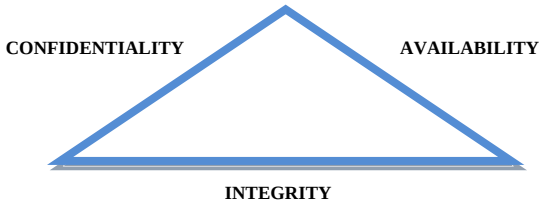

Fig 4: Principles of Network Security

Table 1: Various Security Threats

THREATS	DEFINITION	THREATS
Confidentiality	Confidentiality is defined as a property that ensures only authorized units (users, parties or systems) should have the competency to access the ensconced data.	◆ Man-in-the-middle ◆ Eavesdropping ◆ Sniffer Attack ◆ User Impersonation ◆ IP Spoofing ◆ Elevation of Privileges
Integrity	Integrity means that only authorized entities should have the ability to modify the data, only through authorized means. It is concerned with correctness, completeness and trustworthiness of the data.	◆ Tampering ◆ Data Breaches ◆ Session Hijacking ◆ Software Modification ◆ Impersonation ◆ Sinkhole Attack
Availability	Availability is the property of the system to be usable and approachable by an authorized unit whenever required.	◆ Distributed Denial of Service ◆ Hardware Interruption ◆ Connection Flooding ◆ Job starvation due to viruses or worms ◆ Hardware Theft ◆ Natural Disasters

3. RELATED WORK

Sana Belguith [7] et al proposed a hybrid encryption technique which was an amalgamation of asymmetric and symmetric cryptographic algorithms. In the model, asymmetric algorithm was used to disseminate keys between cloud provider and authorized users and symmetric algorithm was deployed to encrypt the data. Their technique was proved to be faster and more robust than other cryptographic techniques in processing data as the combination provides the brisk performance of symmetric encryption along with adept security of asymmetric encryption, all along sustaining the rights of users to avenue data in an authorized and protected manner.

L. Ertaul [8] et al investigated a handful of radical security concerns of cloud computing and extant defiance to those security threats. The authors discussed various vulnerabilities, threats and data security requirements and standards. They

elaborated numerous security challenges of distinct categories such as information security, network security, general security issues, etc and suggested impeding measures.

Hualgory Tianfield [9] presented a compendious analysis of the challenges and issues of security in cloud environment. In his study, he analyzed impacts of peculiar characteristics of cloud computing, such as multi-tenancy, elasticity and third party control, upon the security arrangements. Moreover, he estimated the exigency of security in cloud in terms of fundamental issues, such as integrity, confidentiality, trust, availability, etc. Additionally, he discussed the taxonomy for security issues in cloud computing.

Hu Shuijing [10] reckoned a few imperative data security issues involved while immigrating to cloud scenarios, and commenced the fundamentals of the schema that addresses the position. He discussed a number of arrangements that exemplify propitious proceedings that addresses the data security, such as encryption, access control and strengthening management. However, his study concluded that the currently, most viable option for mitigation is to clinch that any regulated or sensitive data should not be saved into a public cloud.

Pardeep Sharma [11] et al addressed distinct security issues that emanated due to framework of the service delivery models of a cloud computing system. The authors studied diverse deployment models and key security issues of cloud computing and suggested ways to eliminate various insecurities of cloud.

H.A Dinesha [12] et al proposed a multi-level authentication system which validates the password at disparate levels to successfully access the cloud services. They used n-tier architecture, where n is based on the level of security needed. First level of authentication defined is organization level authentication; second level of authentication is team level authentication. Finally, the last level is user level authentication. The number of levels can be increased or decreased according to the requirement. Major disadvantage of this system is the need to remember all of the passwords.

Pachipala Yellamma [13] et al proffered a rubric for providing secure data storage and security in virtual environment. The authors focus on various security challenges and data storage methods on cloud. They use a public key cryptosystem, namely, RSA for providing security and describe discrete security services, such as key generation, encryption and decryption in virtual environment.

G. Prabu Kanna [14] et al proposed a way to revamp the security of outsourced data on cloud. This is brought about by a competent hybrid encryption and Proxy Re-Encryption (PRE). The data of cloud storage consumer is encrypted before storing them in cloud storage. Encryption is done in two phases, in the first user data is encrypted along with receiver identity. In the second phase the identity and the keyword is encrypted using PRE. Finally, these two cipher texts are combined and sent to the cloud server. The receiver obtains the original message with the private key matching to the identity.

Akshita Bhandari [15] et al proposed a hybrid encryption RSA along with Advanced Encryption Standard (AES) to ensure efficiency, consistency and trustworthiness in cloud servers. The authors use various cryptography concepts during communication along with its application in cloud computing and to enhance the security of cipher text or encrypted data in cloud servers along with minimizing the consumption of time, cost and memory size during encryption and decryption.

A. Ashok Kumar [16] et al postulated a two layer security framework for data storage in cloud environment. The mechanism uses public key cryptography at the first layer and second layer is based on steganography. At the first layer, RSA method is used for key swapping between users and AES for encryption and decryption to make approach computationally adept. The second layer disarranges the encrypted messages in stegad images so that the security is much higher than other individual approaches. The advantage of this mechanism is that processes are computationally facile, so availability of data is unaltered. However, the disadvantage is that the exactitude of RSA for the infrequent instances when P is not relatively prime to n is not yet proven.

4. PROPOSED RESEARCH

Security issues and threats, as discussed above, deteriorate the experience of using cloud technologies. To appease the security requirements of users and vanquish the security issues, attribute based encryption technique is used. We propose a security enhancement system in which the security will be improved at multiple levels. At the first level, an OTP is sent to the user's mobile phone and email-id to preserve authenticity of the user. The OTP and account passwords will ensure that no unauthenticated us user gets access to the data saved on the cloud. On the consecutive levels, at the cloud environment, data provider will encrypt the data with a key and transfer it to Key Generator server and this server will further encrypt the data and provide the private key encrypted back to data provider. User with combination of both, Private Key as well as Public Key, will be able to access the main cloud server and the cloud server sends the user details to data provider and if actual owner of data authenticates user, he would be provided with the key to access the data. The key will only be catered if the user proves to be legit. Along with these, a file compression technique is also used on the cloud server to make sure that the data occupies minimum possible space on cloud and requires minimum bandwidth during the transmission of the data. This technique improves the efficiency of the cloud server while maintaining the integrity of the data as well.

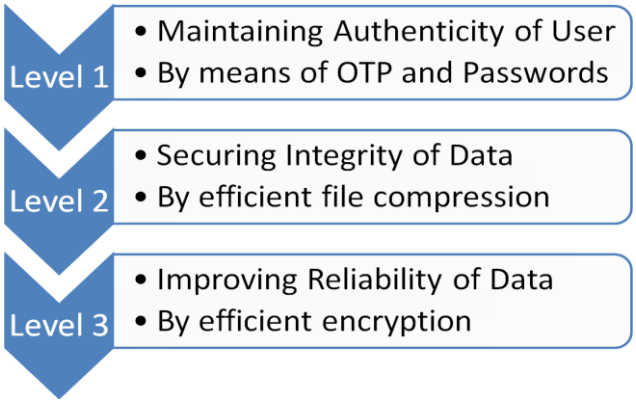

Fig 5: Implemented Security Levels

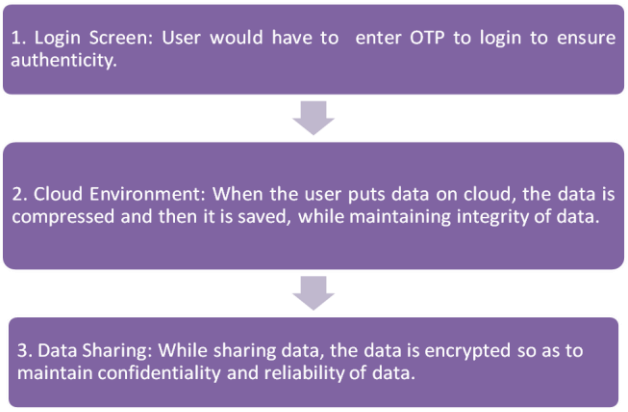

Fig 6: Steps for Security

5. CONCLUSION

Cloud Computing is an ultra-modern technology that is extensively being adapted due to its flexibility, scalability, profitability and increasing accessibility. Despite its advantages, cloud suffers from certain liabilities as well. Cloud environment is an insecure environment which possesses a great threat to privacy, availability, integrity and confidentiality of data. The objective of proposed work is to improve the security of data and make cloud environment more efficient and secure for user experience. In future, the model can be improved by reducing the time complexities of the algorithms used for encryption and compression. The user graphic interface of the model can also be improved for better user experience. In this paper, we discussed basic concepts, various models of cloud computing, and different security issues and threats in cloud computing. We also proposed a model to achieve higher level of security and efficiency in cloud environment. Our model is also advantageous from storage point of view as file compression is done while maintaining the integrity of data. This work can be further enhanced by working on the complexity of the algorithm used and making it more adaptable.

6. REFERENCES

[1] "Azure Microsoft: A beginner's guide", 2017, Available: https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/

[2] Sugandha Nandedkar and Sangeeta Kakarwal, "A Review on Cloud Computing Vulnerabilities," International Journal of Innovative Research in Science, Engineering and Technology, 2014.

[3] P.Samundeeswari, "Cloud Computing Models and its Benefits", International Journal for Research in Science Engineering and Technology (IJRSET) 2015, Volume 2, Issue 10, pp. 6-13, 2015.

[4] Sumit Goyal, "Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review," I.J. Computer Network and Information Security, 2014, pp. 20-29, Published Online February 2014 in MECS.

[5] "Cloud Computing", 2016, Available: http://searchcloudcomputing.techtarget.com/definition/cloud-computing

[6] Saurin Khedia and Nishant Khatri, "A Review on Hybrid Techniques of Security In Cloud Computing," International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 11, November 2014.

[7] Sana Belguith, Abderrazak Jemai and Rabah Attia, **"**Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm," ICAS 2015, The Eleventh International Conference on Autonomic and Autonomous Systems.

[8] L. Ertaul, S. Singhal, and S. Gökay, "Security challenges in Cloud Computing," International conference on Security and Management (SAM), 2010, pp 36–42.

[9] Huaglory Tianfield, "Security Issues in cloud computing," IEEE International Conference on Systems, Man and Cybernetics, October 14-17,2012, COEX, Seoul, Korea.

[10] Hu Shuijing, "Data security: the challenges of cloud computing", Sixth International Conference on Measuring Technology and Mechatronics Automation, January 2014, Hunan, China.

[11] Pardeep Sharma, Sandeep K. Sood, and Sumeet Kaur, "Security Issues in Cloud Computing," International Conference, HPAGC 2011, Chandigarh, India, July 19-20, 2011, pp 36-45.

[12]H.A. Dinesha and V.K. Agrawal,"Multi-level Authentication Technique for Accessing Cloud Services," IEEE International Conference on Computing, Communication and Applications (ICCCA), 2012, pp. 1-4.

[13] Pachipala Yellamma, Challa Narasimham and Velagapudi Sreenivas, "Data Security In Cloud Using RSA, Computing," Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference, July 2013.

[14] G.Prabu kanna and V.Vasudevan, "Enhancing the Security of User Data Using the Keyword Encryption and Hybrid Cryptographic Algorithm in Cloud," International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), March 2016.

[15] Akshita Bhandari, Ashutosh Gupta and Debasis Das, "Secure Algorithm for Cloud Computing and Its Applications," Cloud System and Big Data Engineering (Confluence), 2016 6th International Conference**,** January 2016.

[16] A. Ashok Kumar, Santhosha and A.Jagan, "Two layer Security for data storage in cloud," Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), 2015 International Conference, February 2015.