A Survey on Cloud Computing and Security Challenges to Cloud Computing

Mansi Varshney
Manav Rachna International
Institute of Research and Studies
F-81B, Badarpur, Harinagar Extn,
Jaitpur, New Delhi-110044

Saurabh Raturi
Manav Rachna International
Institute of Research and Studies
H.No-1468 Bankey Bihari Colony
near G.B Public School, Tilpat,
Faridabad, Haryana 121003

Jyoti Verma
Manav Rachna International
Institute of Research and Studies

ABSTRACT
Cloud Computing is a transformative computing paradigm that involves delivering applications and services over the internet using standard access mechanisms through the use of workstations, laptops, smart phones etc [1]. Due to this technology, the expense of computation, application facilitating, content storage and conveyance have been reduced. This paper presents the advantages of using cloud computing, reviewing the several cloud deployment and service models. This paper also analyzes the key challenges and security issues to cloud computing as security is one of the major issues which hamper the growth of cloud. It also provides cryptographic algorithms of data security and a comparative analysis of data security algorithms. It also addresses some methods to minimize these challenges.

Keywords
Infrastructure-as-a-service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), Cloud Computing

1. INTRODUCTION
People have consistently been storing the projects and information that they need onto their computer's hard disk and getting to it at whatever point required. This is known as computing. In cloud computing, computing resources are delivered over the network connection, usually the internet. Instead of deploying local hardware and software, a pool of physical or virtual resources is shared in cloud computing. It sounds like the term 'utility computing', as clients can go into the flexibility of computing resources rather than themselves dealing with the equipment required to create it. Section II covers an overview on cloud computing and also explains some of the advantages of cloud computing. Section III explains about the importance of using clouds. Section IV and V review the building blocks and service models of cloud computing respectively. Section VI deals with the challenges of cloud computing and some ways to overcome them. Section VII reviews some of the security issues in cloud computing. Section VIII covers a brief of cryptographic algorithms. Section IX includes a brief about the different research papers on cloud computing. Finally, the conclusion is given in SECTION X.

2. CLOUD COMPUTING: OVERVIEW
Cloud computing is an effective way to experience direct cost benefits. It has the ability to change a data center from a capital-intensive set up to a variable priced environment. The aim of cloud computing is to expand skylines across organizational limits and this is what makes it different from traditional computing ideas such as "grid computing", "distributed computing", and "utility computing". Cloud

computing is being utilized every day by everything but it isn't realized. Editing documents, sending messages, listening to music, watching movies or TV, playing games or storing pictures and different documents is just conceivable with cloud computing.
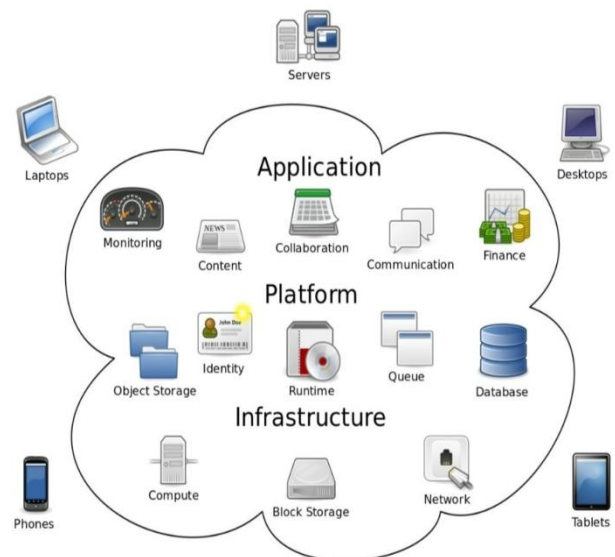

Fig.1 Cloud Computing

The advantages/benefits of cloud computing are

a. As there is no huge cost of hardware hence the cost is very less in cloud computing.

b. Flexibility in capacity which could be turned off, up or down according to the user[2].

c. Availability is for 24*7 i.e it has the accessibility around the globe.

There are many other advantages too like scalability, mobility, data security etc. The software based on cloud offers various advantages to the organizations from all divisions. One of the advantages is the ability to use the software from any device such as laptop, mobile phones etc. Also, clients can exchange their documents and files to different devices in a very reliable and convenient way. It additionally offers large organizations tremendous cost-sparing potential. When the cloud system was not there, organizations were required to buy, build and maintain costly infrastructure and information management technology but now the workers can interact with the cloud online and can easily finish their work in very less time. It is also possible for the organizations to swap their server places

and IT departments for quick internet connections.

3. WHY CLOUD?

a) The main reason of utilizing the cloud by a large number of small scale and large scale business segments and by the people from everywhere throughout the world is that utilization of cloud computing results in the large amount of cost saving. The minimization in the hardware and the software cost and other server resources become possible just because of the cloud computing.

b) It is also possible to use cloud online over the internet and to run all the applications and processes remotely and therefore, eliminating the need of using physical hardware and software.

c) Cloud Computing Service Provider helps in managing the issues like server maintenance, installation of software or hardware, renewal of license etc.

d) Cloud has made it possible to access any data, application, over the internet, whenever and wherever required.

e) Cloud helps in handling data storage and also protects and recovers all crashed or loss data and hence it provides higher security.

4. CLOUD COMPUTING BUILDING BLOCKS

The developing ubiquity of cloud computing has offered various kinds of cloud service deployment models and techniques. Cloud organization models demonstrate how the cloud services are made accessible to clients. The following are the four primary deployment cloud computing models:-

Private cloud: The private cloud is defined as a cloud computing model that offers a secure and distinct cloud based environment and which can be operated by a single client. The underlying pool of physical computing resources is utilized to provide computing power as a service within a virtualized environment. This cloud offers predominant control and security by allowing just a single organization to get to the pool of resource. The arrangement and management of private clouds can be adjusted based on their requirements for acquiring a customized network solution. A private cloud model can help in allocation of resources in a better way within an organization by confirming resource availability to the individual departments/business functions by reacting to the requests in an immediate and adaptable manner.

Public Cloud: The public cloud model is the most perceived model of cloud computing to several purchasers that offers services in a virtualized environment. The pool of shared physical resources is utilized to build the physical resources and the environment can be accessed over a public network that is web or internet.

Public cloud is like a private cloud where the pool of underlying computing resources is limited and creates a distinct cloud platform that is available to just a single association or organization. Services are offered to numerous customers with the same shared framework or infrastructure. Examples of public cloud include AWS, Google Drive.

Hybrid Cloud: A computing environment that includes both a private and a public cloud for sharing the information and applications to perform various functions is known as hybrid cloud.

A client consistently searches for specific efficiencies at certain levels in cloud computing services however public cloud services are more cost proficient and versatile in contrast with private cloud. In the case of hybrid cloud, the efficiencies can be expanded by implementing public cloud services for all the non-critical operations and dependent on private cloud for the critical operations. An example of hybrid cloud includes Netflix.

Community Cloud: A Community Cloud is a multi-tenant platform in which infrastructure is shared between different organizations which may be managed by them or a third party service provider. It allows several companies to share a common platform if they have similar needs and concerns. These clouds are normally based on an understanding between related business associations, for example, banking or educational associations. According to this model, the operating cloud environment may exist locally or remotely. Facebook is an example of community model [3].

5. SERVICE MODEL

Cloud is a scalable service which can be accessed through web connection with a higher transmission capacity. For an organization to choose the best cloud service which can fulfill their needs, it is very important to know the basic difference between the cloud services. Cloud is an expansive service model in cloud computing which covers the best possible online service. The cloud service models are categorize as follow-

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Fig.2 Cloud Deployment Models

Each of these cloud model services have their own intricacy still at the same time are essential to imply a specific cloud service which satisfies the IT needs. These service models are the three main standard models that satisfy their roles.

Infrastructure as a service (IaaS): Infrastructure as a service is a self-service model which allows the users to run their operating systems on the leased servers. This service provides

the architecture and infrastructure. It is basically a pay-as-per use models, therefore, the users need to pay only for the services they actually used. It helps in the cost saving for the users as the users don't have to buy the expensive physical servers and even they need not to concentrate on installing, configuring and managing their software as the cloud service provider deals with all these frameworks. The users also get access to the virtual data center through the internet as it provides all the resources on the virtual environment so that multiple users can access the resources.

Platform as a Service (PaaS): Platform as a Service is a complete development and deployment environment that is made up of a programming language execution environment, an operating system, web server, and database. It extends from cloud-based applications to cloud-enabled applications as it provides an environment to its users where they can build, compile, and run their program and they need not to worry about the hidden infrastructure. The users just need to maintain the applications only.

PaaS is the perfect platform for the software creation as its users can concentrate on building the software part only without worrying about the operating systems and infrastructure. For the development of software, the vendors provide all the necessary tools. The users can simply access the service through the internet.

Software as a Service (SaaS): Software as a Service is a type of service that utilizes the internet to deliver its application and which is managed by a third party vendor, for its users. It is independent of the platform as it is based on the on-demand pay per use of the application software. The users only need to subscribe for the application they want to use and hence the users no longer have to purchase and install the application. The responsibility of installing, operating, and maintaining the software application have been taken by the service provider and thus, free its users from this burden.

Earlier, to use the software, individuals had to buy the software and then have to load it into the device but now the only thing they have to do is to subscribe for the software they want to use. The software can be accessed from anywhere via the internet. This service model guarantees various benefits to its users and to the business organization as well. To reduce the hardware cost, installation and maintenance cost, this model eliminates the need of installing and running the applications on their own computers [4].

6. CHALLENGES

1) Security and Privacy: As in cloud computing, the software and applications are accessed over the internet, therefore, the security and privacy are the main challenges to cloud computing.

These challenges can be reduced by utilizing security applications, encrypted file systems, data loss software [5].

2) Interoperability: It is defined as the process in which the application on one platform is able to incorporate services from the other platform which is becoming possible through web services, but developing such web services is a complex process [6].

Industry standards should be developed so that cloud service providers can design interoperable platforms and can enable data portability to overcome this challenge.

3) Portability: It means that the applications running on one cloud platform when transferred to a new cloud platform, then

it should work correctly without making any changes in design and coding. Since, different cloud providers use different standard languages for their platform, therefore, it is also a challenge to the cloud computing.

It can be minimized through standardization and intermediation.

4) Service Quality: The Service-Level Agreements (SLAs) of the suppliers are insufficient to ensure the accessibility and adaptability. If there is no strong service quality assurance, then the organizations wouldn't prefer to switch to cloud.

It can be resolved by the intervention of standardization which is required to deploy interactive real-time services with high demands on service quality, reliability and predictability on cloud platforms.

5) Computing Performance: For data intensive applications on cloud, there is the need of higher bandwidth but this may result in the higher cost. So, this is the challenge to cloud computing as the low bandwidth does not meet the desired computing performance [7].

6) Reliability and Availability: It is mandatory for the cloud systems to be reliable and robust as most of the businesses are dependent on services provided by third-party. If there is an unreliability of on-demand software then users will not be able to access mail and synchronize data correctly, so the software needs to have a reliability quality factor so that clients can access it under any network conditions.

7) Compliance: At the point when organizations are moving their local data to a cloud they have to agree to specific general body policies if the information is from public sources. Finding a cloud supplier who will follow these strategies is hard to find, or one needs to negotiate on that front.

8) Lack of Resource/Expertise: It is also one of the challenges in cloud computing as it is difficult for the employers to find workers with the skills or abilities they need.

Various organizations are planning to conquer this challenge by employing more workers with cloud computing certifications or skills. Specialists also prescribe providing training to existing staff to help raise them to an acceptable level with the technology.

9) Managing Multi-Cloud Environments: Since most organizations aren't using just one cloud, they are using a multi cloud environment but managing multi cloud environments adds complexity as faced by the IT teams. To overcome this challenge, experts suggested best practices like doing research, training employees, actively managing vendor relationships and re-thinking processes.

10) Migration: If a new application is launched then moving an existing application to a cloud computing environment is very difficult as companies face many problems migrating applications to the cloud have to like time-consuming trouble-shooting, difficulty configuring security, slow data migration, downtime during migration , difficulty syncing data before cutover, etc [8].

7. SECURITY ISSUES

A report shows that although cloud computing configurations provide computer based resources, tools, applications etc which gives greater flexibility to consumers in terms of cost effectiveness, but the report also highlights the security issues with cloud computing and how it has increased in the past

years.

1)   Distributed-Denial-of-Service Attacks (DDoS): It is one of the hacking tactics often used by the hackers. DDoS attacks have greatly increased in viability as the availability of IoT devices, smartphones and many other computing devices have been increased. It prevents the legitimate users from accessing the service as the hackers keep the server busy.

2)   Security and unauthorized access: Although the threat is particularly dangerous with cloud solutions, the main security issue for all systems is employee negligence and employee mistakes. The employees may leave their systems vulnerable to outside threats when they log into the cloud solutions from their devices.

3)   Data Loss and Inadequate Data Backups: If there is inadequate data backups and improper data syncing, then it leads to the threat known as ransomware. What actually ransomware does is that it locks away a company's data in encrypted files and only decrypts their files and allows them to access the data once a ransom amount has been paid. It can be overcome with appropriate data backup solutions.

4)   Phishing and Social Engineering Attacks: These attacks have become popularly common due to the openness of the cloud computing system. The main aim of the phishing and social engineering attack is to acquire the personal information of the user such as credit card number or login credentials. Once the information is acquired, the attacker or malicious user can access the system from anywhere. To avoid these types of attacks, the user should be knowledgeable about these types of attacks.

5)   System Vulnerabilities: The systems that have complex infrastructures and multiple third-party platforms are vulnerable to the attacks. This vulnerability can be easily used against organizations if it becomes known with a third-party system. To overcome this threat, proper patching and upgrade protocols are required in addition to network monitoring solutions [9].

Many of the above security issues can be solved by using data protection service. Cloud data protection solutions protect the data against cyber security threats and also protect the data loss.

8. CRYPTOGRAPHIC ALGORITHMS

There are generally two types of cryptographic algorithms:

- Symmetric Key cryptographic algorithms

- Asymmetric Key cryptographic algorithms

A) Symmetric Key cryptographic algorithms
i) Triple Data Encryption Standard (3DES): As hackers learned to defeat the Data Encryption Standard (DES) algorithm, Triple DES was designed to replace the original DES. Earlier, Triple DES was a widely used symmetric algorithm in the industry but now it is only used for financial services and other industries.

It makes use of three 56 bits individual keys. The total key length is 168 bits but arguably 112 bits.

ii) Blowfish: It is the symmetric cipher flexible encryption method designed to replace DES. It splits messages into groups of 64 bits and then encrypts them individually.

Due to its fast speed and overall effectiveness, it is very popular among the different organizations. It can be found in various software categories like in e-commerce and password

management tools.

iii) Advance Encryption Algorithm (AES): It uses 192 and 256 bits for heavy duty encryption process, although it is extremely efficient in 128 bit form. It is considered impenetrable to all attacks except brute force.

iv) Twofish: It is a symmetric technique in which only one key is needed. The total key length can be upto 256 bits. It is one of the fastest techniques and it can be ideally used in both hardware and software environments. It is freely available therefore, anyone can use it.

B) Asymmetric key cryptographic algorithm

i) RSA (Rivest–Shamir–Adleman): It uses a pair of keys, that's why it is a public-key encryption asymmetric algorithm. The standard for encrypting data is sent over the internet. The result of RSA encryption is that it makes it quite difficult for attackers to break the processing power as it takes quite a bit of time to attackers [10].

ii) Digital Signature Algorithm (DSA): This algorithm uses both the public and private key. The private key is used for the generation of digital signature for a message and that signature is verified by the signer's corresponding public key.

iii) Diffie–Hellman key exchange: To exchange cryptographic keys over a public channel, Diffie–Hellman key exchange method is used. Using this key exchange method, two parties that are unknown to each other can establish a shared secret key over an insecure channel. It is used to secure a variety of services related to the internet.

iv) ElGamal: It is a public key cryptosystem and it is based on the discrete logarithm problem for a group. Every person has a key pair, a secret key and a public key. Given only public key one has to find the discrete logarithm to get the secret key. It helps to exchange sensitive information over an insecure channel eavesdropped by adversary Eve and a digital signature scheme which helps to create digital signatures.

9. LITERATURE SURVEY

Cloud computing offers benefits to companies seeking a competitive edge in today's economy as it mainly focuses on industries, such as banking, healthcare and education which are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources like processing power utilized, transactions carried out, bandwidth consumed, data transferred, or storage space occupied and so on etc. The research paper also deals with the challenges of cloud computing. The organizations are slow in accepting it due to security issues and challenges associated with it [11]. Mohsin Nazir concluded that there will be a major shift towards the cloud in the coming years.

The research paper proposed by Santosh Kumar and Dr. R.H Goudar explains characteristics and applications of several popular cloud computing platforms. It reviews the challenges and issues of cloud computing as security and privacy issues present a strong barrier for users to adapt into cloud computing systems [12]. Santosh Kumar and Dr. R.H Goudar concluded that since cloud computing initiatives have the ability to change IT, therefore, it could affect the enterprises within two to three years.

The research paper proposed by Dr. Uday Salunkhe and Sandeep Kelkar highlights the role of cloud computing in the educational sector and the things which need to be improved. 53% of the institutions provide eBooks which is an advantage for students and changing the environment. 92% of the

institutions use traditional classroom teaching methods and also use video conferences for lecture delivery. 73% of the institute officials are fully aware of Internet and cloud computing technologies. 70% of the institutes have college websites but do not have any mechanism for study material or content delivery. 100% of the institutes use email for collaboration with regulators, students and other stakeholders. From the security aspect 60% of the institutes believe that cloud is somewhat insecure. 45% of the institutes believe that staff motivation will affect their cloud adoption for management education [13]. Dr. Uday Salunkhe and Sandeep Kelkar concluded that cloud computing is a rapidly developing Internet-based computing model.

The goal of cloud computing includes resource utilization, elasticity, minimizing IT cost etc to manage temporary loads. Cloud Computing has various flexible services and deployment models which is also one of the main issues to adopt this computing paradigm. The research paper focuses on the need of privacy and on solutions of various security problems to maintain the trust level of organization for deploying the cloud computing without any hesitation and also need of technical support for elastic scalability to serve by vertical scaling approach which is currently restricted to only horizontal scaling [14]. Suruchee V.Nandgaonkar and Prof. A. B. Raut concluded that virtualization technology plays a major role in accomplishing the goal of cloud computing.

10. CONCLUSION

This paper outlined a survey in cloud computing services focusing on the IaaS, PaaS, SaaS service models and on the various building blocks of cloud computing. Cloud Computing is a new emerging technology having various advantages like scalability, mobility, data security, less cost, disaster recovery etc. Cloud Computing is a future technology with rapid development, however, it is facing some obstacles in its way which hampering it to become more popular i.e it is facing some key challenges which have been discussed in this research paper. One of the main challenges is security in cloud computing which can be solved step by step. One should be aware of how secure their data is and what are the several security threats to their systems which can lead to the leakage of their personal information. So, this paper also outlined some of the cryptographic algorithms which are required for data encryption, authentication and digital signature. Since the development of cloud computing technology is still at an early stage, this research effort will provide a better understanding of the design challenges of cloud computing, and help others for further research in this area.

11. REFERENCES

[1] Pinal V Chauhan, "Cloud Computing In Distributed System," International Journal of Engineering Research & Technology (IJERT) Vol. 1, December- 2012 ISSN: 2278-0181.

[2] Priyanshu Srivastava and Rizwan Khan, "A Review Paper on Cloud Computing," International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X.

[3] Lalit Mohan, Richa Pandey, Sanjeev Bisht and Janmejay Pant, "A Comparative Study on SaaS, PaaS and IaaS Cloud Delivery Models in Cloud Computing," International Journal on Emerging Technologies (Special Issue NCETST-2017) 8(1): 158-160(2017).

[4] Anupama Prasanth, "Cloud Computing Services: A Survey," International Journal of Computer Applications (0975 – 8887) Volume 46– No.3, May 2012.

[5] Gurmeet Singh, Vineet Kumar Sachdeva, "IMPACT AND CHALLENGES OF CLOUD COMPUTING IN CURRENT SCENARIO," International Journal of Social Science & Interdisciplinary Research Vol.1 Issue 10, October 2012, ISSN 2277 3630.

[6] Nazia Majadi, "Cloud Computing- Research Issues and Challenges," Proceedings of the Global Engineering, Science and Technology Conference 2012, Dhaka, Bangladesh.

[7] Adnaan Arbaaz Ahmed, Dr.M.I.Thariq Hussan, "CLOUD COMPUTING: STUDY OF SECURITY ISSUES AND RESEARCH CHALLENGES," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4,April 2018, ISSN: 2278 – 1323.

[8] Faraz Fatemi Moghaddam, Mohammad Ahmadi, Samira Sarvari, Mohammad Eslami and Ali Golkar, "Cloud Computing Challenges and Opportunities: A Survey," 2015 1st International Conference on Telematics and Future Generation Networks.

[9] Moulika Bollinadi and Vijay Kumar Damera, "Cloud Computing: Security Issues and Research Challenges," Journal of Network Communications and Emerging Technologies (JNCET) Volume 7, Issue 11, November (2017).

[10] Priya G , M. Lawanya Shri , M. B. Benjula Anbu Malar ,K. Santhi , M.Deepa, "Security Algorithms in Cloud Computing: A Review," International Journal of Pure and Applied Mathematics Volume 117 No. 7 2017, ISSN: 1311-8080.

[11] Mohsin Nazir, "Cloud Computing: Overview & Current Research Challenges," IOSR Journal of Computer Engineering (IOSR-JCE) ISSN: 2278-0661, ISBN: 2278-8727Volume 8, Issue 1 (Nov. - Dec. 2012), PP 14-22.

[12] Santosh Kumar and Dr. R.H. Goudar, "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey," International Journal of Future Computer and Communication, Vol. 1, December 2012.

[13] Dr. Uday Salunkhe and Sandeep Kelkar, "A Research Paper on "A Study on the Scope of Cloud Computing in Management Education," AIMA Journal of Management & Research, May 2016, Volume 10 Issue 2/4, ISSN 0974 – 497.

[14] Suruchee V.Nandgaonkar, Prof. Raut, "A Comprehensive Study on Cloud Computing," International Journal of Computer Science and Mobile Computing, Vol.3, April- 2014.