ISSN: 0976-3104
ISSUE: COMPUTER SCIENCE

ARTICLE

A DETAILED STUDY OF VARIOUS CHALLENGES IN CLOUD COMPUTING

Arushi Garg[1*], Shruti Suman[2], Mansi Goyal[3], Veena Tayal[4], Prateek Jain[5]

[1,2,3,4] Department of CSE, Manav Rachna International Institute of Research & Studies, INDIA

[5]Accendere Knowledge Management Services Pvt. Lt. INDIA

ABSTRACT

Cloud computing is internet based ("cloud") development and use of computer technology ("computing"). Because of accessibility of diverse services and extensibility for vast areas of computing processes, individual users and organizations convey their data and services to the cloud storage server. The point of demarcation between the responsibilities of the provider and those of the user is denoted by the cloud symbol. The network infrastructure as well as the servers are covered in cloud computing since they lie within its boundary. A set of IT services provided to a customer over a network on lease with the ability to scale up or down their service requirements is called cloud computing. Cloud computing services are usually delivered by a third-party provider who owns the infrastructure. The security issues and challenges associated with cloud computing are making organizations hesitate in accepting it despite potential gains achieved. Nevertheless, of its advantages, the transformation of local computing to remote computing has brought up many security issues and challenges for both the users and providers. One of the major issues that hamper the growth of cloud is security. This paper focuses on existing issues in cloud computing such as security, privacy, reliability and so on.

THE IIOAB JOURNAL

INTRODUCTION

KEY WORDS
Cloud Computing, Challenges, Issues, Models, Security

Cloud computing is a representation for empowering appropriate, on demand network approach to a shared pool of arrangement of computing resources that can be swiftly planning and unconfined with minimal administration effort or service provider communication [1].

Cloud Computing is a different method of commercial computing. It will be extensively used in the nearby future. The fundamental notion of cloud computing is dropping dispensation encumbrance on the customer's terminal. These are obtainable via a fast internet connection. This is a whole new concept that many organizations are adopting as to give their customers more memory space to keep their files. Although this is a sedition technology used worldwide numbered third most used latest technology, this also signifies the growing trend in the market nowadays in IT industry.

In specific, five vital features of cloud computing are clearly articulated in [Fig.1].

Received: 15 Nov 2018
Accepted: 24 Dec 2018
Published: 12 Jan 2019

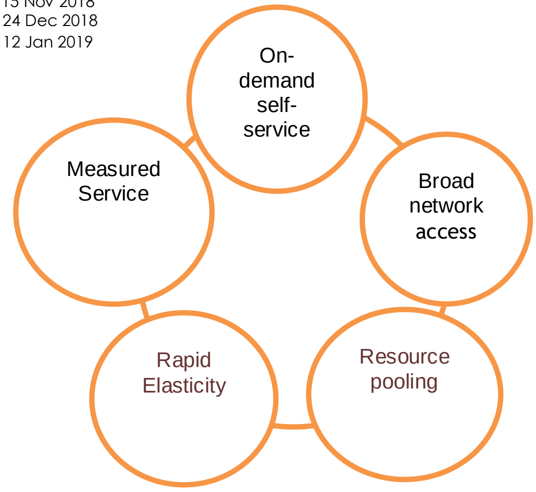


Fig.1: Vital Features of cloud computing.

- On-demand self-service

A user with a prompt necessity at a precise timeslot can benefit computing resources in an involuntary (i.e. convenient, self-serve) manner without resorting to human communications with providers of these properties. [1]

***Corresponding Author**
Email:
arushigarg1997@gmail.com

- Wide-ranging network access

Cloud computing properties are brought over the network and used by numerous applications with mixed platforms located at customer's website.

- Resource Mutualisation

Cloud service provider's resources are 'mutually together' in a determination to aid various customers using virtualization model or perhaps software multi-tenancy.

- Quick elasticity

Resources are instantaneous not persistent, there will be no agreement and in conduct so as to they can be used to scale up whenever they want and scale down to release them.

- Measured Service

As computing resources are mutual and communal by various customers, cloud substructure uses suitable to verify the procedure of the numerous machineries to amount the procedure. [1]

CLOUD COMPUTING AND BUILDING BLOCKS

Service model

There are 4 types of services:

- *Software as a Service (SaaS)*

SAAS is the huge area that holds all the cloud services it provides the customer. It is referred to as "On-demand Software". SaaS is utilized by users through web browser using lightweight computer that has been modified into server –based computers. It achieves standardizationwith respect tovelocity, cost effectiveness, securing the data, availability of data, maintaining it too.Examples are Google Mail, Google Docs, etc. [2]

- *Platform as a Service (PaaS)*

PaaS comes under category of cloud computing services that provide platforms to users for them to develop, run and monitor applications without the difficulty of building and maintaining infrastructure which includes developing and launching an app. So, if we differentiate between these two services it will result in giving solution as- SaaS will only launch fully develop Applications whereas PaaS will lunch both fully developed and in-progress cloud applications. It can be delivered in 3 ways:

- private service,
- public service, and
- private and public software.

Example is Google AppEngine. [2]

- *Infrastructure as a Service (IaaS)*

IaaS is a form of cloud computing service that provide virtual resources to users over the internet. A hypervisor runs the virtual machines as guest machine. It provides high-level APIs for dereferencing various network infrastructure. IaaS is the capability provided to user to provision various fundamental resources so 14 user can run these software.
Example is Amazon's EC2. [2]

Deployment model

Recently, new deployment models have been introduced in Cloud Computing.

- *Private cloud*

The cloud organization is exclusively functional with a single association and is managed by other bodies irrespective of the foundation it is set upon.
The reason behind developing a private cloud are quite many. Following are the reasons:

- Increasing the utility of in-house resources
- Security purposes
- Cost for data transfer from IT infrastructure to public cloud is considerable
- Academics play a major role
- Organization require full access of all activities going on in cloud system. [3]
-

- *Community cloud*

Community cloud refers to sharing of same cloud infrastructure and also its policies behind joining the cloud. It is a viable option as:

- Economic scalability
- Symmetry in form of creating policies.

This cloud can be presented through third party bodies or IT in the following communities. [3]

- *Public Cloud*

Public Cloudis the most used type of deployment model of cloud computing. This type is utilized by many customers. The cloud service provider holds full ownership to public cloud and has its own policies, profit, charging etc. Examples are Amazon EC2, S3, Google AppEngine, and Force.com [3].

IIOAB JOURNAL ISSN: 0976-3104

- *Hybrid cloud*

This cloud model is a combination of two or more clouds by allowing sharing of data and application with other clouds [3].

CHALLENGES IN CLOUD COMPUTING

In previous decades to pass, cloud computing has proved to be a promising business concept the IT industry all over the world currently. Now, IT companies are realizing that by entering the world of cloud computing, they can make most of the profit in their business at a negligible price. But as we know that every advantage has a con tail, which is why in spite of having millions of advantages it lacks the following features that every IT company dreams to have in their cloud computing package in [Fig. 2] [4].
Challenges:

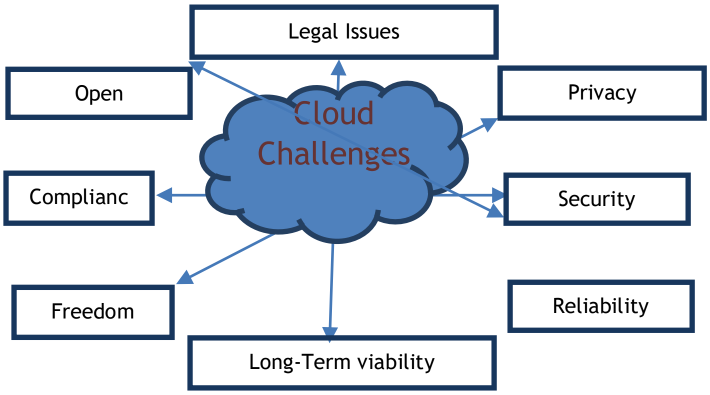


Fig. 2: Challenges in Cloud Computing.

....

- **Security**

Is your data more secure on local hard drive or on high security servers in the cloud that IT companies sell? Some might argue that the data is secure more if it is managed internally, in other hands some says that cloud provides high tech security to users. However, the data that is in cloud is stored in multiple computers. So how is he data safe in cloud? If the hacker access any of these computers, he/she might be able to use our information in any form he/she wants. The IT companies that provide cloud platform must work on providing high security to their customers in order for them to rapidly increase their reputation in the business world [4,5].

- **Privacy**

Customer's personal data might be distributed among different computers rather than stay in one physical location. This might lead to violation of privacy of customer. It may even be possible that the customer may leak information when using the services of cloud [4,5].

- **Reliability**

Cloud servers and resident servers have the exact problems. It means, that the cloud server experiences downtime, interruptions and slowdowns.The only difference is that customer has much larger dependencies on cloud service providers in the cloud computing model [6].

- **Performance and bandwidth cost**

IT companies need to spend more on bandwidth if not on hardware. This will result in low cost for smaller applications but may be quite high foe data-intensive application. We require sufficient bandwidth to deliver intensive and complex data over the network. Due to this, many companies are in line waiting for a reduced cost before switching to cloud [6].

- **Open Standard**

Open standards are very important for viable increase in the growth of cloud in IT companies. Most cloud providers reveal APIs which are well documented and unique too which makes it non-interoperable. Some uses others APIs which are under open standards [6].

- **Compliance**

Using of data requires audit and reporting trails, CSP must allow user to fulfill agreements and regulations. If we manage protection and compliance, it deliversvisionon how an opinionof IT Company can transfer a tight Management and fulfillment of compliance regulations. In conclusion, the customers' requirements are maintained by cloud providers [7].

- **Freedom**

Cloud providers doesn't enable customers to access the data storage. It means that data controls are for cloud computing.Users tend to deny when not given freedom to retain their duplicate copies of data to retain their choice to freedom and secure them too [7].

- **Long-term Feasibility**

One must ensure that all of the data one must put up to not perish. If, so ask your cloud provider as to how can you search the retrieval data back and will be replaceable setup [6,7].

DATA STORAGE AND SECURITY IN CLOUD COMPUTING

We can define cloud security as protection of all the data related to cloud provider as to no unauthorized user can hack it. It is a broader field of security of computer, network and information [8,9].

The major services provided such as a shared resource, identity management, privacy and access control are particular concern. Since more companies are now switching to cloud-based services and the related providers for operations of data, security in vulnerable areas to become priority for cloud computing providers. A study by current review displays that securing of data and privacy of risks are becoming major concern for people who are shifting to cloud computing. Hence, we can say that many complications still exist in cloud computing. Contrarily, a distinct person will have control on security of data and processed on their computers. Additionally, the services and maintenance of data are provided via a vendor where no client/customer are unaware of how will all the processes are working. So, rationally talking, the user will have no control over it. If we talk of data security in cloud, the vendors provide Service Level Agreements to ensure assurance.

CLOUD SECURITY ISSUES

- **Data Security**
  We should secure the data as it is main concern of all the companies as it may hamper their reputation if security is breached. Almost 70% survey tells that security are breached in these IT industries quite easily. [7][8]

- **Refusal of regulating security orders**
  Approximately 40% of the IT industries are concerned as to how to make sure agreement of the company is achieved so that reputation of companies is achieved. If there is a security breach then it will hamper the compliance and result to fines and loss of business contracts. [8]

- **IT services not to control**
  The survey indicates that their fear for loss of control in IT industry can manifest in many ways. Here, data moves to cloud services. [8]

- **IT expertise**
  Almost 40% of industries are not controlling cloud platforms. The reason may be knowledge and IT expertise. [10]

- **Compromised accounts or insider threats**
  30% of survey indicates which accounts are used by SaaS provider and can be compromised in quite methods which is not important here. [10]

- **Continuity in business**
  If a company loses all the accesses of its IT industry, it may seem as it has gone out of business. It can be a rare scenario but it is 30% of the chances. [10] [11]

SECURITY ALGORITHMS

Every user needs a secure communication channel and large data storage over the network. For this purpose the encryption algorithm plays a vital role in the network. It is the fundamental tool for protecting the data. Encryption/Decryption algorithms convert the message into encrypted form using "the key" and only the authorized user or receiver has that key therefore, can decrypt the transmitted message using provided key. Thus it ensures confidentiality, integrity, availability and authentication of the data [Table-1]. There are two types of security algorithm; symmetric key encryption and asymmetric key encryption. [12][13][14]

Table 1: Key used for Encryption/Decryption

Key of comparison	DES	AES	RSA	MD5
Key used for encryption/Decryption	Same key is used	Same key is used	Different keys	Hash function is used for one way cryptography
Key Size	56	128, 192, 256	>1024	128
Performance	Slow	Fast	Fast	Faster

- *RSA (Rivest-Shamir-Adelman)* – Also known as public key algorithm. It is the mostly uses the algorithm- Asymmetric key algorithm, which consists of 2 keys that are:

– Public
– Private

We will use public key is used to encrypt data and is known to everyone and private key is not known to anybody except receiver. The server performs asymmetric key by encrypting a distinctive memo for example, digital signature to enforce authenticity of the sender [15].

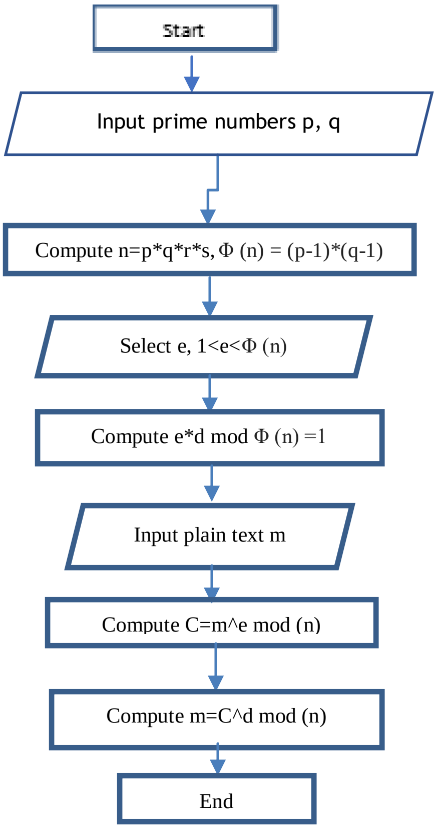


Fig. 3: RSA Algorithm [15].

…………………………………………………………………………………………………

- *DES (Data Encryption Standards)*- DES is a symmetric key block cipher. It was published and accepted by the National Institute of Standards and Technology (NIST).The encryption process is made of two permutations and sixteen Fiestal rounds. DES uses 16 rounds .Each round of DES is a Fiestal cipher. It works by using the same key for encryption and decryption of message, so both the sender and receiver must know and use the same private key .DES uses 64-bit key ,and the length of the key determines the number of possible keys and hence feasibility of attack on the system.

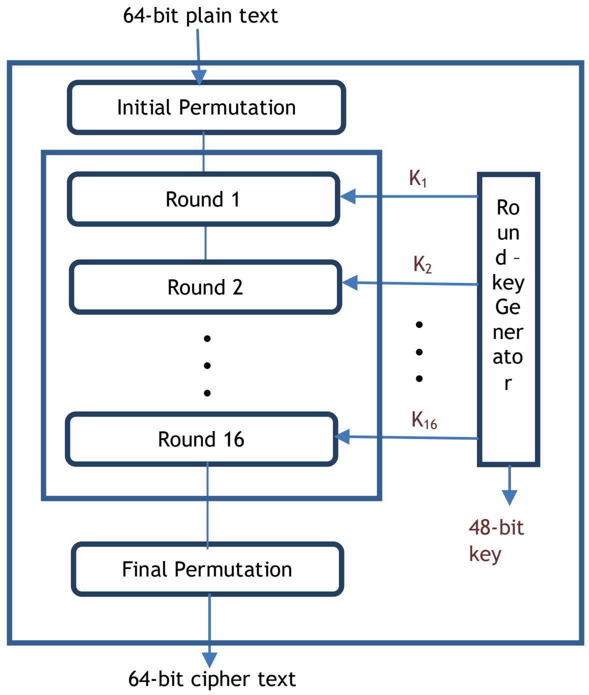
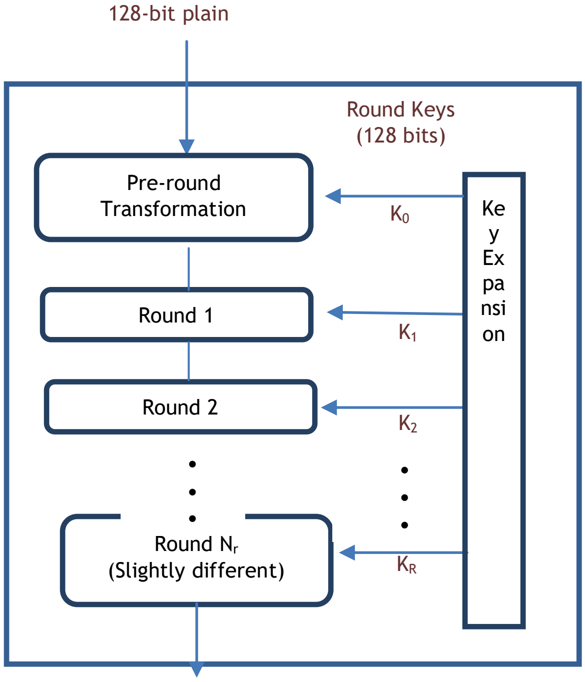


Fig. 4: Data encryption standard.

……………………………………………………………………………………

- **AES *(Advanced Encryption Standard)*** - AES is a symmetric key block cipher which was published by the National Institute of Standards and Technology (NIST).It is also known as non-Fiestal cipher that can encrypt and decrypt a data block of 128 bits. It uses 10, 12, or 14 rounds. The key length, which can be 128, 192, or 256 bits, depends on the number of rounds. It generates the encrypted hash code in highly secure manner which also ensures confidentiality of the message. It works on three broad categories mainly:
  - Security
  - Cost
  - Implementation

  The AES replaced the DES with new and updated features. The techniques involved in this algorithm are so easy and flexible such that they can be easily implemented using cheap processors and also consumes less amount of memory. The symmetric algorithm requires only one encryption and decryption key. It ensures data security for 20-30 years. Allowing worldwide access with no royalties, it has overall easy implementation. [16]



128-bit cipher text

Fig. 5: Advanced Encryption Standards.

……………………………………………………………………………………

- *MD5 (Message Digest Algorithm 5)*- It is the most commonly used cryptographic hash function algorithm with 128 –bit hash value and it can generate variable length message into fixed length output of 128 bits. Even though MD5 is prone to attacks, but still it can be used as a datum to verify and ensure the integrity and authentication of the message transmitted. In MD5 algorithm firstly, the input text provided is broken into chunks of 512 bits blocks and then the text is padded so that its total length is divisible by 512.

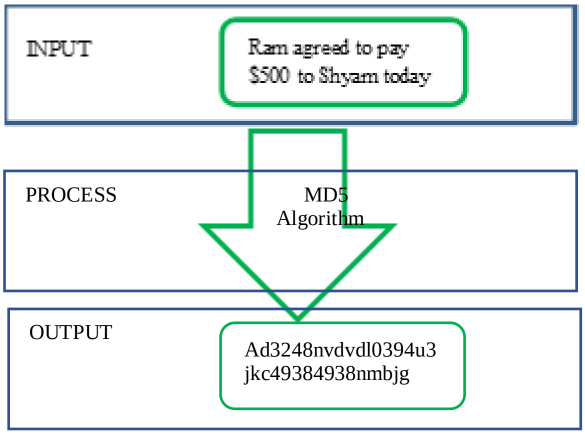

INPUT
Ram agreed to pay $500 to Shyam today
PROCESS
MD5 Algorithm
OUTPUT
Ad3248nvdvdl0394u3 jkc49384938nmbjg

Fig.6: Message Digest 5(MD5).

……………………………………………………………………………………………………..

RECENT TRENDS IN CLOUD COMPUTING

1) **Surge in Demand For Cloud Experts**
   - As many people are adopting to cloud, IT infrastructure requires more experts to become a major competition to its rival business.
   - So, IT manager searches for candidates that have gained experience in cloud platform as improving these skills is becoming a top priority.

2) **Hybridization of technology**
   - Many smaller companies or start-ups have moved to cloud platform permanently but it's a different scenario for larger companies to shift their entire IT operations to cloud based platform, security being an essential issue. [16]
   - So what these large organization do, they partially shift to cloud platform and rest is handled as it was which makes it complex.

3) **Reduced Software Restrictions**
   - This software puts an end to consumer's freedom. It infrastructure often restrict consumer's right to download and application permissions.
   - But the increase in cloud adoption, services allow IT infrastructure to control applications without neglecting user's choices.

4) **Rise of SaaS**
   - To gain successful operations, one must invest heavily in hardware, people and software too.
   - But again cloud adoption has proved to be beneficial as it cuts the operational costs without reducing the profit a business a can earn. [17]

5) **Increased focus on Long Term Relationships**
   Cloud platform has proved that it can run alongside the IT infrastructure and business for the long-term relations in order to gain customer's success.

6) **Rebranding of Service Providers**
   Before cloud was introduced, service providers focused on on-premises software's technical supports.

TECHNIQUES TO SECURE DATA IN CLOUD

- **Authentication and Identity**

Authentication of users and communicating systems is achieved by various means (Cryptography being the most common). Authentication of users happen via various methods [18][19]:

– Passwords, and
– Security token or fingerprint.

Identification of users can be achieved via:

- Fingerprint
- Passwords etc.
-

- **Data Encryption**

We need to use data encryption techniques if we are to store confidential information. Nowadays hackers can bypass passwords and firewalls in a few seconds to access the critical data. An encrypted data cannot be read until and unless it is decrypted with an encryption key.It is a technique of converting plain text into cipher text. Only the receiver will have an encryption key as to read the data provided to him. [18]

- **Information integrity and Privacy**

Cloud computing deliver information and resources to authorized users only. We can achieve integrity by providing communal faith between receiver and sender. We can also achieve authentication, authorization and accountability to ensure that the data is in hands of authorized user. We can secure our data by security Algorithms discussed above – RSA, DES etc. [19]

- **Availability of Information (SLA)**

Availability of resources, in terms of information security, means that the resources to an authorized user must be available whenever he/she needs. So, if the information is unavailable it creates a havoc. We use SLAs to provide information about whether the users have available resources they need or not. We can have a backup plan of resources and crucial information for a way to provide available resources. This will allow the user to have the information even if they are un-available. [19][20]

- **Secure Information Management**

It is the practice of gathering, monitoring and analyzing security related data from logs. A Security Information management System powers that practice. It is sometimes called security event management. It includes log data created from various sources like IDS, IPS routers, servers etc. SIMS will do following activities [20]

- Monitor events
- Display real time view
- Translate event data into common format, XML.
- Aggregate data
- Correlate data

- **Malware-injection attack solution**

Here, number of client virtual machines are generated and stored in a central storage location. Here we use File Allocation Table which consists of various virtual operating systems. This table consists of applications that are run by client. All the cases are monitored and run by hypervisor. We can use IDT for checking integrity. [20]

CONCLUSION

Security issues in the field of cloud computing are active area of research and experimentation. Various issues have been identified one of which is security of user data and applications. Security is always a major concern in open system architectures and needs to be managed effectively. Several cloud computing services are available to achieve security with varying techniques and methods. There are many new technologies emerging at a rapid rate, each with technological advancements and the potential to make human's life easier. However, one must be careful to understand the security risks and challenges posed due their utilization and implementation. In this study, we have discussed key security considerations and challenges which are currently faced in the cloud computing and also specified some techniques to secure data in the cloud. Owing to the issues which are prevalent, a proactive approach to the adoption of the Cloud computing is advised.

Adopting few security measures from user end, can go a long way in maintaining secure files on cloud. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. Cloud Computing security challenges are a part of ongoing research. Various open issues are identified as a future scope.

CONFLICT OF INTEREST

None

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to Dr. Prateek Jain, Accendere Knowledge Management Services., Ms. Veena Tayal, FET, MRIIRS for their valuable comments that led to substantial improvements on an earlier version of this manuscript.

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Stergiou C, Psannis KE, Kim B, Gupta, B. [2018] Secure integration of IoT and Cloud Computing. Future Generation Computer Systems, 78(2): 964-975.

[2] Kumar S, Goudar RH. [2012] Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. International Journal of Future Computer and Communication, 1(4): 356-360.

[3] harma M, Husain S, Zain H. [2017] Cloud Computing Architecture& Services. IOSR Journal of Computer Engineering, 19(2):13-18.

[4] Singh A, Chatterjee K.[2017] Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79:88-115.

[5] Deepthi S, Tulasi V. [2013] A Study of Security Issues and Cloud Models in Cloud Computing. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2(12): 3265-3270.

[6] Zhou MQ, Zhang R, Xie W, Qian WN, Zhou A. [2010] Security and Privacy in Cloud Computing: A Survey, 2010 Sixth International Conference on Semantics, Knowledge and Grids(SKG), 105-112. Doi: 10.1109/SKG.2010.19

[7] Kumar S, Goudar RH. [2012] Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. International Journal of Future Computer and Communication, 356-360.

[8] Dillon T, Wu C, Chang E. [2010] Cloud Computing: Issues and Challenges. 2010 24th IEEE International Conference on Advanced Information Networking and Applications. Doi: 10.1109/AINA.2010.187

[9] Vurukonda N, Rao BT. [2016] A Study on Data Storage Security Issues in Cloud Computing. Procedia Computer Science, 92:128-135.

[10] ICCSEA 2012, Wyld, D. C, Zizka, J, Nagamalai, D. (Eds.). [2012]. Advances in computer science, engineering & a4pplications: Proceedings of the second International Conference on Computer Science, Engineering & Applications (ICCSEA 2012), May 25-27, 2012, New Delhi, India. (Advances in computer science, engineering & applications.) Berlin: Springer.

[11] Stallings W. [2005] Cryptography and Network Security, Prentice Hall, 4th Ed, 2005.

[12] Khan SS, Tuteja, RR. [2015]. Security in Cloud Computing using Cryptographic Algorithms. International Journal of Innovative Research in Computer and Communication Engineering, 3(1): 148-154.

[13] Vijayapriya M. [2013] security algorithm in cloud computing: overview. International Journal of Computer Science & Engineering Technology (IJCSET), 4 (9): 1209-1211.

[14] Yang JF, Chen ZB. [2010] Cloud Computing Research and Security Issues. 2010 IEEE International Conference on Computational Intelligence and Software Engineering (CiSE), 10.1109/CISE.2010.5677076

[15] Pellegrini A, Bertacco V, Austin T. [2010] Fault-based attack of RSA authentication. 2010 Design, Automation & Test in Europe Conference & Exhibition. Doi: 10.1109/DATE.2010.5456933

[16] Sumitra. [2013] Comparative Analysis of AES and DES security Algorithms , International Journal of Scientific and Research Publications, 3(1): 1-6.

[17] Suresh KS, Prasad KV. [2012] Security Issues and Security Algorithms in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, 2(10): 110-114.

[18] Jakimoski K. [2016] Security Techniques for Data Protection in Cloud Computing. International Journal of Grid and Distributed Computing, 9(1):49-56.

[19] Angadi AB, Angadi AB, Gull KC. [2013] Security Issues with Possible Solutions in Cloud Computing-A Survey, IJARCET, 2(2): 302-311.