IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 2, February 2020

Review on Data Security in Cloud Computing Environment

Mr. S. Hendry Leo Kanickam M.Sc., M.Phil., B.Ed,.[1], N. Agnas Clementsiya[2], R.Manikandan[3]

Assistant Professor, Dept of Information Technology, St. Joseph's College Tiruchirappalli, India[1]

M.Sc., CS Student, Dept of Information Technology, St. Joseph's College Tiruchirappalli, India[2]

M.Sc., IT Student, Dept of Information Technology, St. Joseph's College Tiruchirappalli, India[3]

Abstract: Cloud computing is a computing technique, where a large group of systems are connected through private or public networks, where data owner can store his data on the remote systems and frees from storage burden and uses the data on-demand, anytime, everywhere. As a Cloud data user does not possess direct control of his data, security is one of the few challenging issues which need to be addressed. Security in Cloud computing can be addressed in many directions such as. Authentication, integrity, confidentiality and many more. Data integrity (or) correctness is a issue where there may have some unauthorized alteration in the data without consent of data owner. Hence, data storage security in cloud computing is of the utmost importance nowadays. In this paper, we summarize some encryption-decryption algorithms which is used to secure the user's data in a cloud environment using a cloud simulation toolkit. Cryptography is caring about the confidentiality of data in the loud. Cryptography these days is a combination of algorithm types:

Symmetric Key Algorithm (AES)
Asymmetric Key Algorithm (RSA)

Keywords: Cloud Computing, Data Security, RSA

I. INTRODUCTION

Cloud computing is latest trend in IT world. It's Internet-based computing, whereby shared resources, package and information, square measure provided to computers and different devices on-demand, just like the electrical grid. This cloud model is comprises the three service models, and four deployment models. The 'Cloud' is a virtualization of resources and the Cloud Computing brings with it many benefits to the end user. These include [1]:

- Access to a huge range of applications without having to download or install anything.
- Applications can be accessed from any computer and from anywhere.

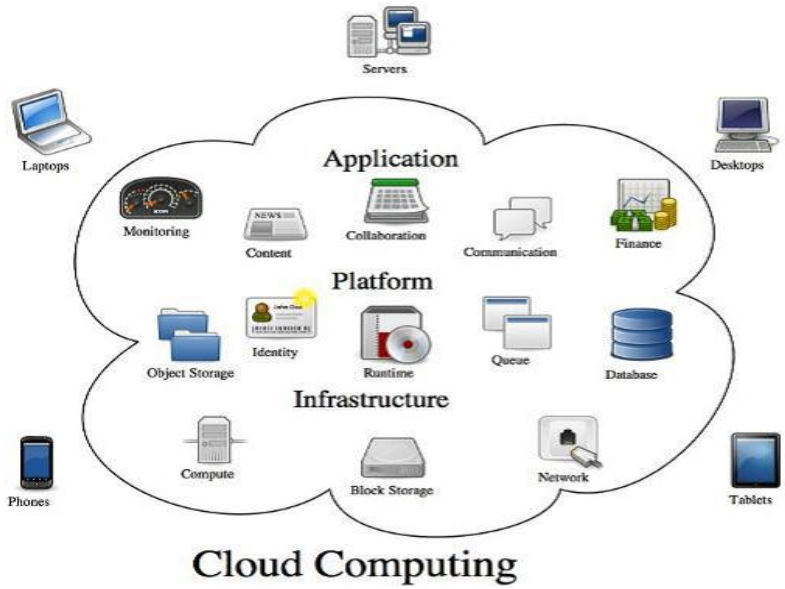


Fig.1 Structure of cloud computing

DOI 10.17148/IJARCCE.2020.9210

- Users can avoid expenditure on hardware and software; only using what they need.
- Companies can share resources in one place.
- Consumption is billed as a utility with minimal upfront costs.
- Scalability via on-demand resources.

The paper is any is organized as under: Section I provides the info security .Section II provides the literature review. Section III classification of cloud computing, Section IV contains security, trust privacy and problems and temporary description of mitigation steps and solutions for these problems. Section V includes security model and experimental results and Section V offers conclusion and future work of this analysis.

II. LITERATURE SURVEY

To secure the cloud security goals of the data include three points namely (CIA):
• Confidentiality
• Integrity and
• Availability
Encryption is divided into two types of algorithm symmetric and asymmetric algorithm. In the symmetric algorithm it use a private key for encryption and the same key is used for decryption. And in asymmetric it uses the public key for encryption and private key is distributed to all using of the private key decrypt the data [5].
And there are plenty amount of security issues for cloud computing and many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.

Data Encryption standard: DES is a block-cipher. It use the 56 bit key and 64 bit blocks DES has a complex set of rules and data. It has quick hardware implementations and slow software implementations. DES takes a 64 bit plain text and creates 64 bit cipher text at decryption side. It uses two permutation initial permutation and final permutation and 16 Feistel rounds. Each round use a different 48 bit round key [6].

RSA: RSA is Asymmetric encryption algorithm it means that public key is distributed to all for encryption and private key is used to decryption .The key size is 1024 bits. In the RSA modular exponential is used for encryption and decryption. It uses two exponents a and b where a is public key and b is private key [5].

Data storage correctness is some time more generally referred as data integrity verification is one of the major Cloud security problems. Data can be altered by the unauthorized entity without intimating to data owner. How the data owner make sure that his data has not been modified by other intruders (or may be by the Cloud provider itself, accidently or intentionally). So detecting such kind of unlawful activities on the data is an utmost priority issue. Data storage correctness schemes can be divided into two categories. The two categories are as follows [7]:

1) Without Trusted Third Party (TTP) and
2) With TTP, based on who makes the verification. As in traditional network security, we try to protect the confidentiality of data.

III. ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING

3.1 Cloud Service Model

The Cloud Service Models are as follows [2]:

1) Software as a Service (SaaS): The capability provide to consumer is to use the provider applications running on a cloud infrastructure. The application are accessible from the various client devices through a client interface, such as a web browser (e.g., web-based email), or a program interface.

2) Platform as a Service (PaaS): The capability of providing a consumer satification is to deploy onto the cloud infrastructure to the consumer-created or acquired applications are created for using programming languages, libraries, services, and some of the tools supported by the provider.

3) Infrastructure as a Service (IaaS): the capability of provision process, storage, networks, and different elementary computing resources wherever the consumer is ready to deploy and run an absolute package, which can including operating systems and applications.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 2, February 2020

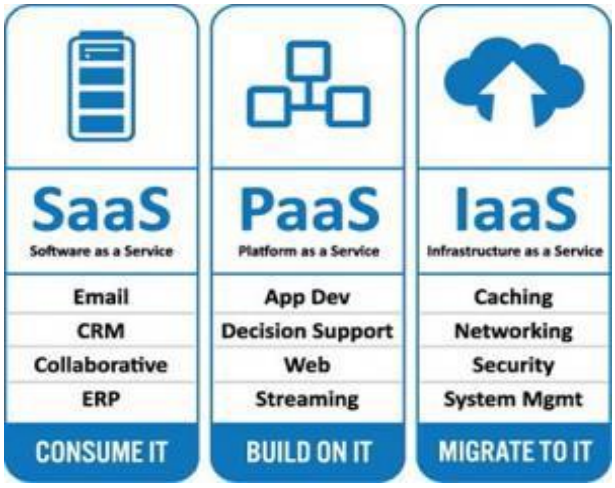


Fig.2 services offered by cloud computing

3.2 Cloud Deployment Model:

The Cloud Deployment Models are as follows [3]:

1) Public cloud: The cloud infrastructure is provision for open use by general public. It can be managed, operated by a business, academic, or government organization, or some combination of them. It exists in premises of the cloud provider.

2) Private cloud: The cloud infrastructure is exclusive use by a single organization comprising multiple consumers (e.g., business units). It can be owned and managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

3) Hybrid cloud: It have two or additional distinct cloud computing infrastructures (private, community, or public) that stay distinctive entities, however are sure along by the standardized (or) proprietary of the technology. Allow to knowledge and application movability (e.g., cloud brusting for load balancing between clouds).

4) Community cloud: The cloud infrastructure is provision for exclusive use by a specific community of consumers organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may owned, managed, and operated by one or more of the a third party, or some combination of them, and it may exist on or off premises.

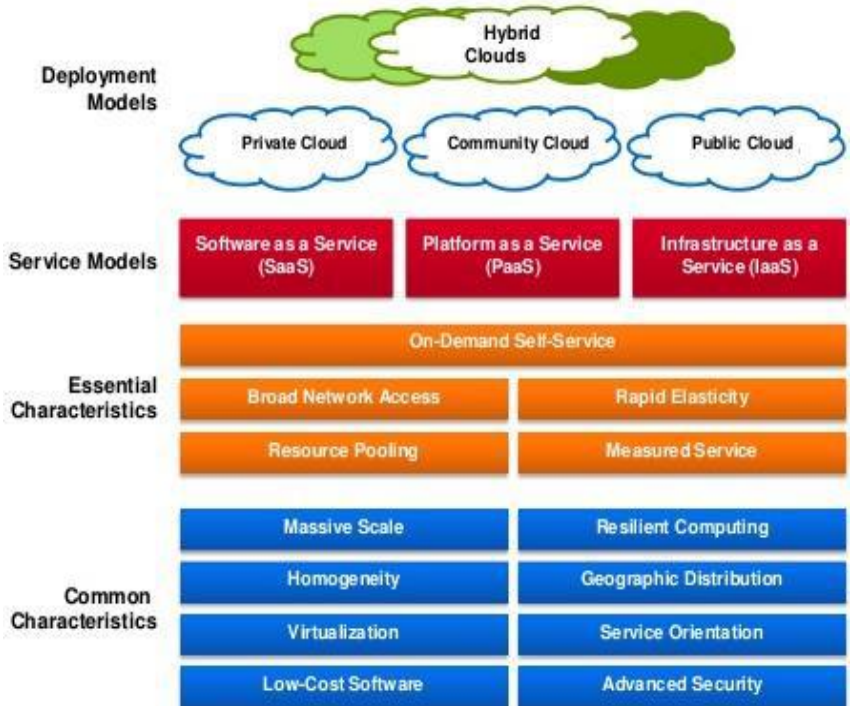


Fig.3 converged infrastructure

DOI 10.17148/IJARCCE.2020.9210

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 2, February 2020

3.3 Storage of Security Concern in Cloud Computing:

The security concerns in cloud computing is as follows 4]:
Security concern #1: With the cloud model management physical security is lost.
Security concern #2: Company has violated the law (risk of data capture by (foreign) government).
Security concern #3: Service incompatibility
Securityconcern#4: Who controls the encryption/ decryption keys? Logically it should be the customer.
Security concern #5: Guaranteeing the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions.
A common customary to make sure knowledge integrity doesn't yet exist.
Security concern #6: Users must keep up to date with application improvements to be sure they are protected.
Security concern #7: Some government rules have strict limits on what knowledge regarding its voters will be hold on and for a way long, and some banking regulators require that customer's financial data remain in their home country.
Security concern #8: The dynamic and fluid nature of virtual machines can build it troublesome to keep up the consistency of security and make sure the auditability of records.
Security concern #9: Customers may be able to sue cloud service providers if their privacy rights are violated. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties.

IV. ISSUES IN CLOUD COMPUTING

Cloud computing is extremely promising for the IT applications; but, there are still some issues to be solved for private users and enterprises to store information and deploy applications within the cloud computing surroundings.

One of the foremost important barriers to adoption is information security, that is in the course of problems together with compliance, privacy, trust, and legal matters. The role of establishments and institutional evolution is getting ready to privacy and security in cloud computing. Information security has systematically been a serious issue in IT field. It becomes significantly serious within the cloud computing surroundings, as a result of information are scattered in several machines and storage devices together with servers, PCs, various mobile devices like wireless or networks and smartphones.

Data security within the cloud computing is a lot of difficult than data security within the ancient info systems. To form the cloud computing be adopted by users and enterprise, the security considerations of users ought to be corrected 1st to form cloud surroundings trust worthy. The trustworthy surroundings is that the basic requirement to win confidence of users to adopt such a technology. Before the data security problems are mentioned, the functions of cloud computing are analyzed first. Cloud computing is additionally called on-demand service. within the cloud computing surroundings, there is a cloud service supplier that facilitates services and manages the services. The cloud supplier facilitates all the services over the web, whereas finish users use services for satisfying their business desires then pay the service supplier consequently.

4.1. Reverse Caesar Cipher

One of the simplest examples of the substitution cipher is the Caesar cipher. It is used by Julius Caesar to communicate with his army. Caesar is considered to be one of the first person to have ever employed encryption for the sake of securing messages. The futher enhanced of the original three places shifting of the character in Caesar cipher uses modulo twenty six arithmetic encryption key that is greater than twenty six in the alphabet.

$$En(x) = (x+n) \bmod 26$$

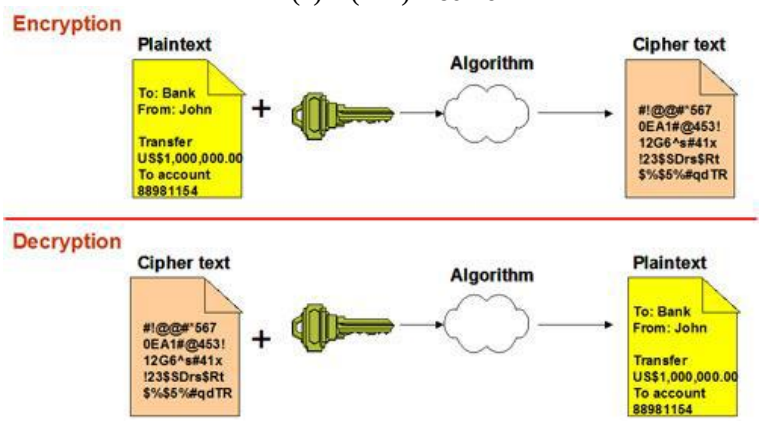


Fig.4 Encryption/Decryption process

The most weakness of this cipher is simplicity of its encryption and decryption algorithms; the system can be deciphered without knowing the encryption key. It can be easily broken by reversing encryption process with simple shift of alphabet ordering.

$$Dn(x) = (x-n) \bmod 26$$

The earliest caesar cipher method include the main drawbacks is plaintext and key is used only 26 alphabets. This paper[6] overcome the above problem to plaintext is used case sensitive, numbers and special characters in order of ASCII full of characters (256 char). This proposed method providing the inverse of Caesar cipher that supports a more security for the data compared with the earliest Caesar cipher.

Encryption Algorithm:

1. Split the letter of the plaintext.
2. Assign the position (i) of the letter.
3. Generate the ASCII values of the Plain text letter.
4. Assigned same Key value is taken as a key.
5. To apply the below given formula: E = (p + k + i) , where, p – Plaintext, k – key, i – Position.
6. Generate the ASCII characters for the corresponding decimal value in the result from the above given formula. This would be the cipher text.

Decryption Algorithm:

1. Generate the American Standard Code for Information Interchange value of the cipher text character.
2. Here the same encryption key used.
3. Assigned a position (i) of the cipher text.
4. To apply the below given formula: D = ((c – k – i) + 256) % 256
   where, c – Cipher text, k – key, i – Position.
5. Generate the ASCII characters for the corresponding decimal value. This would be the original plaintext.

4.2 Example

Encryption:

Let, the character is “c”. Now according to the steps we will get the following:

1. ASCII of “c” is 99 in decimal.
2. Assign a fixed key value is 10.
3. Assign the position (i) is 0.
4. Apply the following formula, Where E = (p + k + i) % 256
   = (99 + 10 + 0) % 256 = 109
5. As per the algorithm the cipher text will be “m”.

Decryption:

After encrypting “c” and “m” as the cipher
text. Now according to the decryption algorithm try to get back the original text i.e. “c”.

1. 109 is the value for ASCII cipher text character “m”.
2. Here, Same key “10” is used.
3. Here, position (i) “0” is used.
4. The formula is applied for ASCII value 109 of the cipher text character and key 10.
   D = ((c – k – i) + 256) % 256 = ((109-10-0) + 256) % 256
   = 99
5. “c” was the ASCII character of the decimal 99. Character “c” will be the original plaintext.

4.3 Advantages

- The algorithm is very simple in nature.
- The users can easily encrypt and decrypt the combination of alphabets, numbers and special characters efficiently.
- It is case sensitive.

V. RIVEST SHAMIR ADLEMAN (RSA)

5.1 Introduction

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first described it in 1977. By securing the data, unauthorized access isn’t allowed. User data is encrypted first and after it is stored in the Cloud. When required, user places a request for data to the Cloud provider; Cloud provider authenticates the user and delivers the data.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 2, February 2020

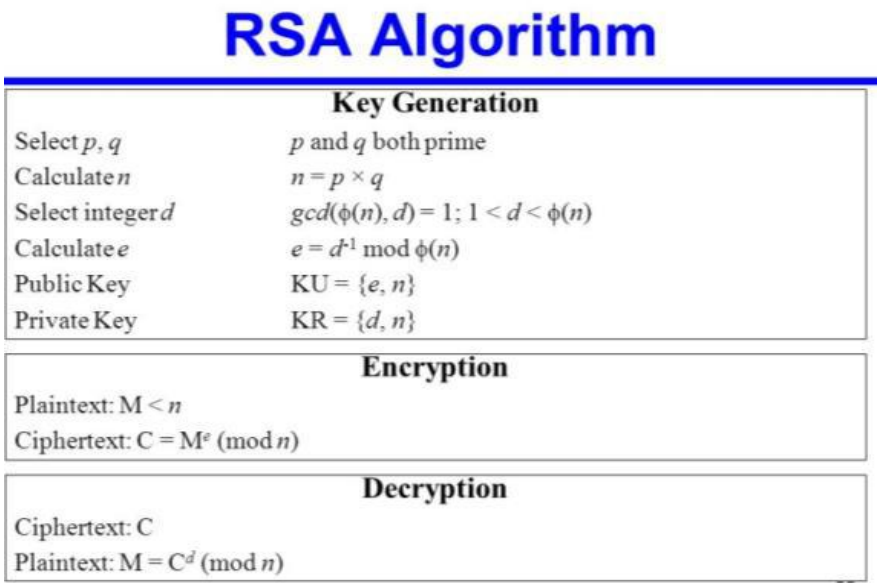
RSA is a block cipher algorithm, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In the Cloud computing, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, the encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with Public-Key, it can be decrypted with the corresponding Private-Key only.
RSA algorithm involves three steps:
1. Key Generation
2. Encryption
3. Decryption

5.2 Algorithm

Key Generation- Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

1. Choose a two distinct prime numbers a and b.
For security purposes, the integers a and b
Are chosen at random and should be of
similar bit length.
2. Compute n = a * b.
3. Compute Euler's totient function, Ø(n) =
(a-1)* (b-1).
4. Choose a integer e, such that 1 < e < Ø(n) and
greatest common divisor is e, Ø(n) is 1. Now
e is released as Public-Key exponent.
5. Now determine d as follows: d = e-1(mod
Ø(n)) i.e., d is multiply inverse of e mod
Ø(n).
6. d is consider as Private-Key component, so that d * e = 1 mod Ø(n).
7. The Public-Key consists of a modulus n and the public exponent e i.e, (e, n).

8. The Private-Key consider as modulus n and the private key exponent d, which must be kept secret key i.e, (d, n).



Encryption- Encryption is the process of converting original plain text (data) into cipher text (data).
1. Cloud service provider should give or transmit the Public-Key (n, e) is to the user who wants to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text (data) C is calculated using, C = me (mod n).
4. These cipher text or encrypted data is now stored with the Cloud service provider.

DOI 10.17148/IJARCCE.2020.9210

Decryption- Decryption is the process of converting the cipher text (or) data to the original plain text(or)data.

1. The cloud users request the Cloud service provider for the data.
2. Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e, C.
3. The Cloud user can decrypts the data by computing, m = Cd (mod n).
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

VI. CONCLUSION

Cloud computing is a way of leveraging technology in the Internet to consume software or other IT services on demand. User can share processing power, storage space, bandwidth, memory, and software. With cloud computing, we shared the resources and so the costs. User can pay as they go and only use what they need at any given time, keeping cost to the user down. Cloud computing is a business model as well. Providers of cloud computing solutions are software, hardware, platform, storage providers, deliver their offerings over the Internet. There are no shrinked wrapped boxes containing discs or hardware for you to buy and set up yourself. Cloud providers are charge monthly recurring fees based on your usage. Cloud computing is a collection of computing software and services available from a decentralized network of servers.

The term “cloud” was long been as used as a metaphor for the Internet, and there are many popular services and Web sites which you may already be enjoying, without being aware that they are cloud-based. Social networking sites, Web-based email clients like Gmail and Yahoo, Wikipedia and YouTube, and even peer-to-peer networks like Skype or Bit Torrent are all applications that run in the cloud. In other words, there is no one centralized location or organization that controls them, and nothing is required to utilize them besides a Web browser and an Internet connection. Enterprise cloud computing is for the business world. Instead of purchasing and installing the physical infrastructures are necessary to run software programs, a business instead consumes resources on a software-as-a-service basis. Running individual applications are such as Microsoft, SAP, or Oracle will require hardware as well extensive infrastructure to support it: office space, power, networks, servers, storage, cooling, and bandwidth, not require to mention it, the experts needed to install and run them.

Cloud relies on trusted computing and cryptography. Number of cloud platforms are available now in educational as well as in enterprises circle. Cloud computing offers a lot of streamlined, simplified solution to this complexity and the capital expenditure it necessitates. There is no doubt that cloud computing has bright future.

REFERENCES

[1]. Mythry Vuyyuru, Pulipati Annapurna, K.GanapathiBabu, A.S.K Ratnam, “An Overview of Cloud Computing Technology”, July 2012, International Journal of Soft Computing and Engineering (IJSCE).
[2]. Sandha, M.Ganaga Durga,” Study on Data Security Mechanism in Cloud Computing”,IEEE conference no-33344.
[3]. Peter Mell, Timothy Grance, “The NIST Definitionof Cloud Computing”, National Institute of Standards and Technology, September 2011.
[4]. Kalyani D. Kadam, Sonia K. Gajre, R. L. Paikrao,“Security issues in Cloud Computing”, 2012, National Conference on Innovative Paradigms in Engineering & Technology.
[5]. Neha Jain and Gurpreet Kaur ‘Implementing DES Algorithm in Cloud for Data Security” VSRD International Journal of CS
[6]. William Stallings, Cryptography and Network Security: Principles and Practices, Fifth edition.
[7]. Vasu Raju, Raj Kumar, and Anand Raj, “Techniques for Efficiently Ensuring Data Storage Security in Cloud Computing”,
[8]. Sajjan R.S, Vijay Ghorpade and Vishvajit Dalimbkar, ‘A Survey Paper on Data security in Cloud Computing’, International Journal of Computer Sciences and Engineering.
[9]. Prof. Swarnalata Bollavarapu Asst Prof, Dept of Computer Engg., Nikhil Kamath,’ Review on Data Storage Security in Cloud Computing’
[10]. Prince Jain, “Security Issues and their Solution in Cloud Computing”, ISSN (Online): 2229-6166.
[11]. Monjur Ahmed and Mohammad Ashraf Hossain, “Cloud Computing and Security Issues in the Cloud”, International Journal of Network Security & Its Applications (IJNSA)
[12]. Aized Amin Soofi, M. Irfan Khan, Fazal-e-Amin,“A Review on Data Security in Cloud Computing”. International Journal of Computer Applications (0975 – 8887).
[13]. F. A. Alvi1, B.S Choudary ,N. Jaferry, E.Pathan, “A review on cloud computing security issues & challenges”.
[14]. Manisha Thakur, Dr. Neeru Bhardwaj,“A Review Paper on Cloud Computing & Security Issue”, International Journal of Computer Science and Mobile Computing, ISSN 2320–088X.
[15]. Rahul K.Morghade, and Sonal Honale, “Data Storage Security and Privacy in Cloud Computing”. http://ijcrst.in/(available
[16]. S.Hendry Leo Kanickam, Dr.L.Jayasimman, Dr.A.Nisha Jebaselli, “ A Survey on Layer wise Issues and Challenges in Cloud Security”, IEEE Xplore , ISSN : 978-1-5090-5573-9/16, DOI 10.1109/WCCCT.2016.49 , pp . 168-171.December 2016. (Scopus indexed)
[17]. S.Hendry Leo Kanickam, Dr.L.Jayasimman,”Cloud Computing Security: Multilevel Classified Survey on Attacks and Security Concerns”, International Journal of Computer Sciences and Engineering, ISSN:2347-2693, pp 155-159 , March 2018. (UGC Approved Journal)