CRYPTOGRAPHIC ALGORITHMS ARE USED IN CLOUD COMPUTING FOR SECURITY: A STUDY

Dr. G. RamaSubba Reddy[1] **S. Santha Kumari[2]** **M. Roshini[3]**
[1,2]Associate Professor,Dept. of CSE, Mother Theresa Institute of Engineering & Technology, Palamaner.
[3]Assistant Professor, Dept. of CSE, Mother Theresa Institute of Engineering & Technology, Palamaner.
Email: subbareddy1227@gmail.com[1] ,shanthakumarissk@gmail.com[2] ,roshini.mohammad@gmail.com[3]

Abstract: Cloud computing is the technology for providing the computing services such as servers, storage, database, and networking etc over the internet on pay per use pattern. It is more popular in today's era as it helps in cost reduction associated with computing. Although it is one of the most prominent technology for such kind of services, the limitation of the technology is the "Data Security and Integrity" in the environment. Cloud computing is one of the latest technology trend of the IT trade for business area. Cloud computing security converged into a demanding topic in the sector of information technology and computer science research programs. Regardless of the fact that cloud computing offers great advantages to the end users, there are several challenging issues that are mandatory to be addressed. It offers an on demand and scalable access to a shared pool of resources hosted in a data centre at providers' site. The cloud computing is a way to deliver IT services on demand and pay per usage, and it can stores huge amount of data. But until now many companies don't wish to use cloud computing technology due to concerns about data secrecy and protection. So we need cryptographic algorithms that can provide a highly secure communication, data integrity and authentication, along with the non-repudiation communication and data confidentiality. It reduces the overheads of up-front investments and financial risks for the end-user. In This paper discusses about symmetric key cryptographic algorithms DES,3DES,AES,RC and Asymmetric key cryptographic algorithms RSA,ECC,Diffie-Hellman,DSS.

Keywords: Cloud computing, confidentiality, cryptographic algorithms, data integrity, DES, AES, RSA, EC.

I . INTRODUCTION

Distributed computing is circulated design with incorporate server. The Cloud processing is web depend innovation which give figuring administrations as Infrastructure as administrations (Iaas), stages as administration (Paas) and Software as Service (SaaS) to the client. The client does not require learning or mastery to control the foundation of mists; it gives just deliberation. It very well may be used as an administration of an Internet with high versatility, higher throughput, nature of administration and high registering force. Distributed computing suppliers convey basic online business applications which are gotten to from servers through internet browser .As assets are use, they are estimated and installment is made based on the usage of the administrations to the CSP (Cloud Service Provider)[14].

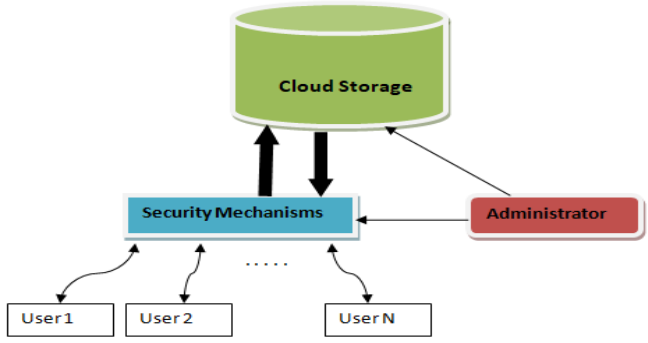

Figure 1: Cloud Storage

The system model of distributed storage comprises of four layers: stockpiling layer which stores the information, essential administration layer which guarantees security and solidness of distributed storage itself, application interface layer which gives application benefit stage, and access layer which gives the entrance stage. The fundamental distributed storage condition spoke to as beneath:

Distributed computing has increased colossal prominence as of late. By redistributing calculation and capacity prerequisites to open suppliers and paying for the administrations utilized, clients can savor upon the upsides of this new worldview. Distributed computing

furnishes with a similarly lower-cost, adaptable, an area autonomous stage for dealing with customers' information. Contrasted with a conventional model of figuring, which utilizes committed in-house framework, distributed computing gives remarkable advantages in regards to cost and dependability. Distributed storage is another financially savvy worldview that goes for giving high accessibility, unwavering quality, enormous adaptability and information sharing. Notwithstanding, re-appropriating information to a cloud specialist organization presents new difficulties from the points of view of information accuracy and security. Throughout the years, numerous information honesty plans have been proposed for ensuring redistributed information.

Distributed computing has picked up a ton of prevalence, which is mostly because of the accompanying reasons : (a) Cloud figuring has dispensed with the overhead of arranging from the client, giving assets that are accessible on-request, self-benefit, and the capacity to scale as indicated by prerequisites. (b) Cloud registering has disposed of in advance duty by the end clients. Pay-as-you-go show has enabled organizations to begin little and increment their registering assets just when required [11].

There are numerous information protection worries in distributed computing. Mistaken disclosure of an information utilized in organizations in cloud to outsiders is one of the real issues that have been found. Encryption ought to be appropriately utilized and the crypto calculations incorporate AES, RSA, DES, and 3DES. In this paper, we depict about utilizing crypto calculations in order to expand security concern. Cloud Security can be guaranteed by client validation, information trustworthiness, Secured information exchange and by Cryptography. There are assortments of cryptographic calculations which can be actualized in order to guarantee security in the cloud. The two kinds of calculations are Symmetric and Asymmetric encryption key calculations. Symmetric contains calculations like DES, AES, 3 DES and Blowfish calculation. Topsy-turvy contains calculations like RSA, Diffie-Hellman Key Exchange. Symmetric key and deviated key calculations is utilized to encode and decode the information in cloud [3].

2. CLOUD COMPUTING

Service Class	Main access & Management Tool	Service Content
SaaS Software As A Service	Web Browser	Cloud Applications Social Networks, Office Suites, CRM, Video Processing
PaaS Platform As A Service	Cloud development Environment	Cloud Platform Programming languages, Frameworks, Mashups editors, Structured data
IaaS Infrastructure As A Service	Virtual Infrastructure Manager	Cloud Infrastructure Compute servers, Data Storage, Firewall, Load Balancer

Figure 2:The Cloud Computing Stack

2.1 CLOUD SERVICES

The different services, being provided in cloud computing, are classified into three categories.

- ***Infrastructure as a service (IaaS):*** Is the delivery of computer architecture over internet. It involves the use of remote computers(O.S , database , middle ware , applications) and storage.
- ***Software as a service (SaaS):*** Is the delivery of Applications (e.g., CRM or ERP) as a service to end users over internet through browsers.
- ***Platform as a service (PaaS):*** Is the delivery of application development and deployment platform (e.g., Pega) as a service to developers over internet through browsers, who use the platform to build , deploy and manage SaaS applications.

2.2 CLOUD TYPES

2.2.1 Public Clouds

Public cloud means no access restrictions can be applied and no authorization and authentication techniques can be used, which are accessible on internet from a minor party, which detached assets and charges its clients on the basis of utility. describes the conventional meaning of cloud computing that is accessible, effective ways and means, Cloud organization is possessed and accomplish by a supplier who suggest its retune to public domain. E.g. Google, Amazon, Microsoft offers cloud services via Internet.

There are different benefits of public cloud model.

- Cost Effective
- High Scalability
- Reliability
- Flexibility
- Location Independence

2.2.2 Private Clouds

Private cloud can be owned or leased and managed by the organization or a third party and exist at on premises or off premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems

There are different benefits of private cloud model.

- High Security and Privacy
- More Control
- Improved Reliability

2.2.3 Community Clouds

Community clouds are shared by several organizations and support a specific community that has shared concerns. Such has security requirements, policy, mission and compliance considerations. These are mainly considered under enterprise cloud computing. For example OpenCirrus formed by HP,Intel,Yahoo and others.

2.2.4 Managed Clouds

Managed clouds arise when the physical infrastructure is owned by physically located in the organization's data centers with extensions of managements and security control plane control by the managed service provider.

2.2.5 Hybrid Clouds

A synthesis of at least two cloud organization models, connected in a way that information exchange happens between them without influencing one another. These mists would regularly be made by the undertaking and the executives obligations would be part between the endeavor and the cloud supplier. In this model, an organization can layout the objectives and requirements of administrations [6].A cross breed cloud contains resources from both private and open suppliers will turn into the requested decision for big business For instance, for general registering venture could chooses to make utilization of outside administrations, and its own server farm's includes it possess information Centre's. Half and half cloud show has number of preferences .

There are distinctive advantages of private cloud show.

- Scalability
- Security
- Flexibility
- Coast efficiencies

2.2.5. Service Providers of Cloud Computing

There are many cloud computing providers available in industry. Few companies are leading in this is listed below [4].

- Amazon Elastic Compute Cloud (EC2)
- Microsoft Azure Services Platform
- Google App Engine
- Salesforce.com
- Akamai EdgePlatform
- IBM Computing on Demand (CoD)
- Rackspace Cloud
- Terremark
- NetSuite

3. SECURITY ISSUES IN CLOUD COMPUTING

The security issue with mists is that the information might not have control of the information is set. As though client needs to exploit the cloud, client must guarantee the sheltered system and furthermore use the asset portion and booking given by mists. The anchored information trade is significant for any system; so it is essential to consider security and protection when structuring and utilizing cloud administrations. Distributed computing is extended approach to cover security issues, concerns and difficulties for Data Security in Cloud.

3.1 Cloud Privacy And Confidentiality

Privacy is characterized as the delicate data isn't unveiled to unapproved people, procedures, or gadgets .The specialist organization knows where the clients' secret information is situated in the distributed computing Systems. When the customer have information to the cloud there ought to be some certification that entrance to that information may be restricted to the approved access. Unseemly access to delicate information by cloud work force is another hazard that can present potential danger information in distributed computing. Assuredness ought to be given to the customers to appropriate practices in security approaches and methods to guarantee the cloud clients for the information wellbeing. Cloud specialist organizations should actualize systems to guarantee information trustworthiness. The cloud supplier should make the customer mindful of what specific information is facilitated on the cloud. it might be important to have correct records with respect to what information was set in an open cloud, when it required, what virtual recollections (VMs) and capacity it lived on when it was handled, such information respectability prerequisites exists, that the root and authority of information or data must be kept up so as to avert altering or to keep the presentation of information past the concurred domains .

3.2. Data Location And Relocation

Distributed computing offers a high level of information versatility. Information versatility is at an abnormal state then the dangers and issues increment numerous folds

particularly shoppers don't generally know the area of their information. At the point when an endeavor has some delicate information that is kept on capacity gadget in the Cloud, clients need to know the area of information and furthermore wish to determine required area. The authoritative assention, between the Cloud supplier and the buyer information should remain in a specific area or live on a given known server, cloud suppliers should assume liability to guarantee the security of frameworks and give powerful verification to protect clients' data. Information is at first put away at a fitting area chosen by the Cloud supplier. In any case, usually moved starting with one place then onto the next. Cloud suppliers have contracts with one another and they utilize every others' assets. For instance, messages, photos transferred to Face book can live anyplace on the planet and Face book individuals are commonly not concerned. They may likewise wish to determine a favored area (e.g. information to be kept in the UK) at that point requires a legally binding understanding between the Cloud specialist co-op and the customer.

3.3 Data availability:

It alludes to a procedure in which information is made accessible wherever it is relied upon to be utilized by end client and

the application. It guarantees the event and accessibility of the information in typical and also in the catastrophe recuperation activities. The accessibility of cloud innovations can be expanded by making web get to accessible however the client is subject to the assets accessible in the restricted time span [9].

3.4 Storage, Backup and Recovery

When you choose to move your information to the cloud the cloud supplier ought to guarantee satisfactory information versatility stockpiling frameworks. At any rate they ought to have the capacity to give RAID (Redundant Array of Independent Disks) stockpiling frameworks albeit most cloud suppliers will store the information in different duplicates crosswise over numerous free servers. Most cloud suppliers ought to have the capacity to give alternatives on reinforcement administrations which are positively vital for those organizations that run cloud based applications so that in case of a genuine equipment disappointment they can move back to a prior state.

4. CRYPTIGRAPHIC ALGORITHMS USED IN CLOUD COMPUTING FOR SECURITY

Cryptographic algorithms are broadly divided into Symmetric key cryptography and Asymmetric key cryptography. Now we will discuss various cryptographic algorithms are used in cloud computing for security.

CRYPTPOGRAPHIC ALGORITHMS	
SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS	ASYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS
Data Encryption Standard(DES)	*RSA*
Triple Data Encryption Standard(3DES)	*Elliptic Curve*
Advanced Encryption Standard(AES)	*Diffie-Hellman Key Exchange*
Rivest Cipher(RC)	*Digital Signature Standard(DSS)*
Blowfish And Twofish	*Elgamal Cryptographic Algorithm*

Table 1: Classification of Cryptographic algorithms

4.1 TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use.

- **Symmetric Key Cryptography:** It is also known as Secret key cryptography or conventional key cryptography. Uses a single secret key for both encryption and decryption. Basically this cryptography used for privacy and confidentiality [2]
- **Asymmetric Key Cryptography:** It is also known as public key cryptography. In this one key used for encryption and another one for decryption. Basically this cryptography used for authentication, non-repudiation, and key exchange [2].

4.1.1 Symmetric Key Cryptography Algorithms

In this paper, we now discuss Data encryption standard, triple DES, Advanced Encryption standard, Rivest Cipher and Blowfish.

4.1.1.1 Data Encryption standard

The most by and large used encryption contrive relies upon the Data Encryption Standard got in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology , as Federal Information Processing Standard 46 . The computation itself is suggested as the Data Encryption Algorithm (DEA).7 For DES, data are encoded in 64-bit squares using a 56-bit key. The computation changes 64-bit commitment to a movement of endeavors into a 64-bit yield. Similar steps, with a comparative key, are used to pivot the encryption.

Whatever the advantages of the case, DES has flourished and is commonly used, especially in cash related applications. In 1994, NIST reaffirmed DES for

government use for an extra five years; NIST endorsed the usage of DES for applications other than the affirmation of portrayed information. In 1999, NIST issued another type of its standard that showed that DES should be used only for legacy structures and that triple DES be used [22].

4.1.1.2 Triple DES

Triple DES utilizes three individual keys with 56 bits each. The aggregate key length means 168 bits, yet specialists would contend that 112-bits in key quality is increasingly similar to it. Notwithstanding gradually being eliminated, Triple DES still figures out how to make a reliable equipment encryption answer for money related administrations and different enterprises.

4.1.1.3 Advanced Encryption Standard

The Advanced Encryption Standard (AES) is the computation trusted as the standard by the U.S. Government and different affiliations. Regardless of the way that it is to an extraordinary degree capable fit as a fiddle, AES moreover uses keys of 192 and 256 bits for bad-to-the-bone encryption purposes. AES is, as it were, pondered impervious to all attacks, aside from creature control, which attempts to unravel messages using each and every possible blend in the 128, 192, or 256-piece figure [22]. All things considered, security specialists trust that AES will in the long run be hailed the accepted standard for encoding information in the private division.

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/3
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/1
Number of Rounds	10	12	
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/1
Expanded Key Size (words/bytes)	44/176	52/208	6(

Table 2: AES Parameters

4.1.1.4 RC2

Ron Rivest developed the RC2 algorithm in the late 1980s as a replacement for DES. RC2 encrypts data in 64-bit blocks and has a variable key size of 8 to 128 bits in 8-bit increments. Lotus Development requested Rivest's help in creating RC2 for the company's Lotus Notes software. Because a large part of an encryption algorithms strength lies in the length of its keys, researchers now consider RC2 to be too easily compromised.

4.1.1.5 Blowfish and Twofish

Security analyst Bruce Schneier built up the symmetric calculation "Blowfish" in the mid 1990s (Reference 3). As with RC2, Blowfish splits messages up into equivalent estimated 64-bit squares and encodes the squares. Its key sizes go from 32 to 448 bits. Schneier discharged Blowfish as an open space calculation, uninhibitedly accessible to anybody needing to encode information. Trying to enhance Blowfish, he later created Twofish, which utilizes 128-piece obstructs keys to 256 bits in length. Twofish is one of the quickest settled square calculations presently accessible, and however it has hypothetical vulnerabilities, nobody has yet broken it.

4.1.2 Asymmetric key Algorithms

Now we discuss about Asymmetric key Algorithms are RSA, Elliptic Curve, Diffie-hellman key exchange, Digital signature standard and Elgamal cryptographic algorithm.

4.1.2.1 RSA

One of the first successful responses to the challenge was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978 [RIVE78].5 The Rivest-Shamir-Adleman (RSA) scheme has since that time reigned supreme as the most widely accepted and implemented general-purpose approach to public-key encryption.

The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 21024.We examine RSA in this section in some detail, beginning with an explanation of the algorithm. Then we examine some of the computational and cryptanalytical implications of RSA[22].

4.1.2.2 Elliptic Curve Cryptography

The addition operation in ECC is the counterpart of modular multiplication in RSA, and multiple addition is the counterpart of modular exponentiation.To form a cryptographic system using elliptic curves, we need to find a “hard problem” corresponding to factoring the product of two primes or taking the discrete logarithm.

4.1.2.3 Diffie-Hellman Key Exchange

The First Published Public-Key Algorithm Appeared In The Seminal Paper By Diffie And Hellman That Defined Public-Key Cryptography [Diff76b] And Is Generally Referred To As Diffie-Hellman Key Exchange.A Number Of Commercial Products Employ This Key Exchange Technique.

The Purpose Of The Algorithm Is To Enable Two Users To Securely Exchange A Key That Can Then Be Used For Subsequent Encryption Of Messages.The Algorithm Itself Is Limited To The Exchange Of Secret Values.

The Diffie-Hellman Algorithm Depends For Its Effectiveness On The Difficulty Of Computing Discrete Logarithms. Briefly, We Can Define The Discrete Logarithm In The Following Way. Recall From Chapter 8 That A Primitive Root Of A Prime Number As One Whose Powers Modulo Generate All The Integers From 1 To P-1 .That Is, If Is A Primitive Root Of The Prime Number , Then The Numbers Are Distinct And Consist

Of The Integers From 1 Through P-1 In Some Permutation.

A Mod P, A^2 Mod P, Á , A^{p-1} Mod P

For Any Integer B And A Primitive Root A Of Prime Number , We Can Find A Unique Exponent Such That

$B = A^i$ (Mod P) Where $0<=I<=(P - 1)$

The Exponent Is Referred To As The **Discrete Logarithm** Of For The Base , Mod .We Express This Value As . See Chapter 8 For An Extended Discussion Of Discrete Logarithms [22].

4.1.2.4 Digital Signature Standard

The National Institute of Standards and Technology (NIST) has distributed Federal Information Processing Standard FIPS 186, known as the Digital Signature Standard (DSS). The DSS makes utilization of the Secure Hash Algorithm (SHA) depicted in Chapter 12 and presents another computerized mark system, the Digital Signature Algorithm (DSA).The DSS was initially proposed in 1991 and overhauled in 1993 in light of open input concerning the security of the scheme.There was a further minor update in 1996. In 2000, an extended form of the standard was issued as FIPS 186-2, therefore refreshed to FIPS 186-3 of every 2009. This most recent form additionally fuses advanced mark calculations dependent on RSA and on elliptic bend cryptography. In this area, we talk about the first DSS calculation.

4.1.2.5 Elgamal Cryptographic System

In 1984, T. Elgamal announced a public-key scheme based on discrete logarithms, closely related to the Diffie-Hellman technique [ELGA84, ELGA85]. The ElGamal2 cryptosystem is used in some form in a number of standards including the digital signature standard (DSS). As with Diffie-Hellman, the global elements of ElGamal are a prime number q And α , which is a primitive root of . User A generates a private/public key pair as follows:[22]

1. Generate a random integer X_A, such that $1 < X_A < q - 1$.
2. Compute $Y^A = \alpha^{X_A} \bmod q$.
3. A's private key is X_A; A's pubic key is $\{q, \alpha, Y_A\}$.

Any user B that has access to A's public key can encrypt a message as follows

1. Represent the message as an integer M in the range $0 \le M \le q - 1$. Longe messages are sent as a sequence of blocks, with each block being an intege less than q.
2. Choose a random integer k such that $1 \le k \le q - 1$.
3. Compute a one-time key $K = (Y_A)^k \bmod q$.
4. Encrypt M as the pair of integers (C_1, C_2) where

$$C_1 = \alpha^k \bmod q; \; C_2 = KM \bmod q$$

User A recovers the plaintext as follows:

1. Recover the key by computing $K = (C_1)^{X_A} \bmod q$.
2. Compute $M = (C_2 K^{-1}) \bmod q$.

4.2 Applications of Asymmetric Key Cryptographic Algorithms

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
Digital Signature Standard	No	Yes	No

Table 3: Applications of Asymmetric Key Cryptographic Algorithms

5 CONCLUSION

The purpose of this study was to review and analyze data encryption for improving privacy of data in cloud computing. This paper proposed better approaches for security the data by using various algorithms proposed for encryption in cloud computing.

REFERENCES

[1] P.S.V. Sainadh,U.Satish Kumar2,S.Haritha Reddy " Security Issues in Cloud Computing " published in International Journal for Modern Trends in Science and Technology Volume: 03, Special Issue No: 01, February 2017 ISSN: 2455-3778.

[2] Archana Singh Parmar, Monika Sharma, " Improving Data Storage Security in Cloud Computing using Elliptic Curve" ,published in International Journal of Engineering Science and Computing, April 2017, Volume 7 Issue No.4

[3] Rishav Chatterjee, Sharmistha Roy, "Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud" published in International Journal of Engineering Science and Computing, May 2017, Volume 7 Issue No.5.

[4] Vishal R. Pancholi , "A Study on Services Provided by Various Service Providers of Cloud Computing" published in Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 6 (2017) pp. 1725-1729

[5] Amritpal Singh, Rajdavinder Singh Boparai," A Review on Big Data and Cloud Computing Security" published in International Journal of Engineering Science and Computing, May 2017, Volume 7 Issue No.5.

[6] T. Deepa , Dr. Dhanaraj Cheelu, " Load Balancing Algorithms in Cloud Computing: A Comparative Study" published in International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 6, Issue 1 January 2017

[7] Priya dhir, Sushil Garg, " Survey on Cloud Computing and Data Masking Techniques " published in International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 6, Issue 4 April 2017.

[8] Sheik Saidhbi and Dr. Komati Thirupathi Rao, "A Modern Approach in Cloud Computing Storage by Using Compression and Crypto Mechanism" published in International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 9 (2017) pp. 1815-1818.

[9] Shweta Singh "Cloud Computing: Security Issues & Solution" published in International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 6 (2017), pp. 1419-1429.

[10] Jaspreet Singh and Deepali Gupta " An Smarter Multi Queue Job Scheduling Policy for Cloud Computing" published in International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 9 (2017) pp. 1929-1934.

[11] Dr. Amit Chaturvedi , Akanksha Kapoor, Dr. Vikas Kumar, " A review of homomorphic encryption of data in cloud computing" published in International Journal of Computer Trends and Technology (IJCTT) – Volume 43 Number 2 – January 2017.

[12] Robin Khunger, Pawan Luthra, Bindu Bala " EA Based Approach for Resource Allocation in Cloud Computing" published in International Journal of Engineering Development and Research, Volume 5, Issue 2 | ISSN: 2321-9939.

[13] Harpreet Kaur, Dr. Manish Mahajan, Nitika Sharma 'Evaluation of Scheduling Mechanisms in Cloud Computing" published in International Journal of Modern Computer Science (IJMCS) ISSN: 2320-7868 (Online) Volume 5, Issue 2, April, 2017.

[14] Akshat Ajabrao Uike, Dr. M. A. Pund " An Overview of Cloud Computing: Platforms, Security Issues and Applications" published in International Journal of Science Technology Management and Research Volume 2, Issue 5, May 2017 ISSN (online): 2456-0006.

[15] Prabhleen Kaur Soul , Sunil Saini "Data Security Approach in Cloud computing using SHA" published in International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 04 Issue: 06 | June -2017.

[16] G. Kishore Kumar, Dr. M. Gobi "Survey on Mobile Cloud Computing [MCC], its Security & Future Research Challenges" published in International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 04 Issue: 06 | June -2017.

[17] Harshil Mehta, Vivek Kumar Prasad and Dr. Madhuri Bhavsar "Efficient Resource Scheduling in Cloud Computing" published in International Journal of Advanced Research in Computer Science Volume 8, No. 3, March – April 2017, ISSN No. 0976-5697.

[18] Mythreyee s,poornima Purohit,Apoorva D.R " A Study on Use of Big Data in Cloud Computing Environment" published in International Journal of Advance Research, Ideas and Innovations in Technology, Volume3, Issue3, ISSN: 2454-132X.

[19] Amr Tolba "Organizing Multipath Routing in Cloud Computing Environments" published in International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.

[20] André Müller1 , André Ludwig and Bogdan Franczyk "Data security in decentralized cloud systems – system comparison, requirements analysis and organizational levels" published in Journal of Cloud Computing: Advances, Systems and Applications, DOI 10.1186/s13677-017-0082-3,2017.

[21] Saad Khan, Simon Parkinson and Yongrui Qin ," Fog computing security: a review of current applications and security solutions",published in Journal of Cloud Computing: Advances, Systems and Applications , DOI 10.1186/s13677-017-0090-3,2017.

[22] William Stallings," Cryptography and Network Security Principles and Practices", Fourth Edition,Nov16,2005.

Author's Biography:

Dr. G. RamaSubba Reddy received his Ph.D in Computer science & Engineering from Sunrise University. He received his M.E in Computer Science & Engineering from Sathyabama University, Chennai. Presently he is working as an Associate Professor and Head of the Department in Computer Science & Engineering, Mother Theresa Institute of Engineering & Technology. Palamaner, Andhra Pradesh. His current research focus is on IoT, Data mining and Cloud computing.

Mrs. S. Santha Kumari received her M.Tech in Computer Science & Engineering from Dr.MGR Educational and Research Institute (M.Tech), Chennai.Presently she is working as an Associate Professor, Department of Computer Science & Engineering, Mother Theresa Institute of Engineering & Technology. Palamaner, Andhra Pradesh, INDIA. Her current research focus is on Cloud Computing.

Mrs. M. Roshini received her M.Tech in Computer Science & Engineering from JNTUA Ananthapuramu. Presently she is working as an Assistant Professor, Department of Computer Science & Engineering, Mother Theresa Institute of Engineering & Technology. Palamaner, Andhra Pradesh, INDIA. Her current research focus is on Image processing.