ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

A Review on Security Threats and Cryptographic Solutions in Cloud Computing

Varsha K[1], Rachel Mathias[2]

Under Graduate Student, Dept. of CS&E, St Joseph Engineering College, Vamanjoor, Mangaluru, India[1,2]

ABSTRACT: Cloud Computing is one among the emerging trends in technology. It delivers various web-based services such as storage, software, databases, servers and more depending on the user's need with the support of virtualization. As the user can access data anywhere from the cloud storage using Internet, maintaining security and confidentiality of data becomes a matter of concern.
This paper emphasizes the issues regarding the security and privacy of data stored in the cloud and the counter-measures taken, mainly, cryptography to overcome those threats.

KEYWORDS: Cloud computing, Virtualization, Security threats, Cryptography, Key Management, Data.

I. INTRODUCTION

Cloud computing, basically, is a form of Internet-based computing which delivers on-demand computing resources, everything from applications to data centers and servers over the Internet on a pay for use basis.Cloud-based applications run on distant computers "in the cloud" that is owned and operated by others and that connect to users' computers via the Internet and usually, a web browser, thus reducing the complexity of storage space foreach software.Some of the benefits include increased efficiency, reliability and flexible costs. But along with these benefits come certain drawbacks of the cloud based services, namely, data security. The cloud environment provides data accessibility anywhere when connected to the Internet. This might lead to unauthorized access of data or information.
Therefore, it's important to understand the four key components of data security: availability, integrity, confidentiality, and traceability.
1) Data availability: The data continues to be available in normal as well asdisastrous conditions. It is implemented by data storage redundancy, network optimization and more.
2) Data integrity: It refers to the assurance of overall completeness, consistency and accuracy of data.It ensures that the data is maintained in its original state i.e., intact and unchanged.
3)Data confidentiality: This means providing authorized access to data. The privacy is maintained by data encryption. Hence, information is available or disclosed only to authorized individuals, entities, or IT processes.
4) Data traceability: It is the ability to track and verify the data, transactions, communications, or documents.

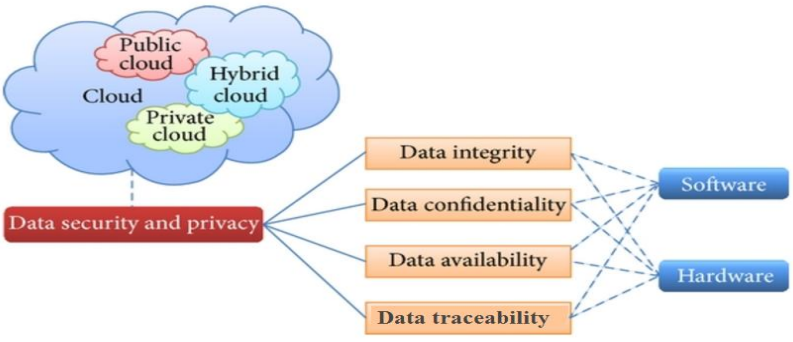

Fig 1: Components of data security system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Thus, in order to preserve the secrecy and integrity of data, a technique called cryptography is used.Cryptography is the encryption of data using different cryptographic algorithms and techniques. A cryptosystem uses 3 algorithms, one each for key generation, encryption and decryption to cipher and decipher the data.

II. RELATED WORK

In [4] authors have discussed about the various security threats that have become a barrier for cloud adoption and also and encryption methods for security in cloud. In [11] authors have used three encrypt techniques AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption. In [14], the author studied about homomorphic encryption and decryption, and how to improve the security using the modified RSA algorithm. In [16] the authors explored data security of cloud in cloud computing by implementing digital signature and encryption with elliptic curve cryptography. They did a detailed study on elliptic cryptography and digital signature generation. In[18] the authors evaluated the performance of the encryption and decryption of each technique used in communication systems, Visual Basic simulation program that encrypt and decrypt data were developed, written and tested. Different data block size were captured and plotted against total time response taken during data encryption using Microsoft Excel. The graph result showed the superiority of RSA and AES algorithms over other algorithms in terms of the processing speed and time. And analysis was made based on the graph result obtained on each data encryption technique.

III. CLOUD SECURITY ISSUES

The cloud is growing rapidly and the past decade has seen an explosion in the popularity of cloud computing. Even though cloud offers a number of benefits, a lack of data safeguards and compliance standards makes security the largest hurdle to leap.While this is no reason to avoid using cloud-based solutions, it is important to be aware of them especially when choosing a supplier. Let us look into some of the most prominent security threats and concerns facing the business and companies moving to the cloud.

1. Data breaches

Data breach (also termed as data leak) threats exist regardless of whether data is stored internally or on cloud. Some cloud services may be more vulnerable to potential attacks and the hijacking of data due to new methods of attack such as "*Man-in-the-Cloud"*. This takes advantage of synchronization services to access and extract data, compromise files or attack end-users. While a cloud provider will implement security measures to reduce the risk of data breaches, but due to the vast amount of data stored on cloud servers, providers become an attractive target. It is important to keep in mind that ultimately, organizations are responsible for protecting their own data in the cloud.A breach can have serious legal and financial consequences depending on the sensitivity of data exposed. Breaches involving health information, trade secrets, and intellectual property can be more devastating.When a data breach occurs, companies that have made use of cloud services may incur fines, or they may face lawsuits or criminal charges.

2. Data loss

Many companies store their sensitive data in the cloud data storage including intellectual property. When a cloud service is breached, cyber criminals gain access to this sensitive data. This may have regulatory consequences. Data loss can have a huge impact financially, operationally and even legally as data loss may result in the failure to meet compliance policies or data protection requirements.Preventing data loss is not solely the responsibility of the cloud provider. If the relevant encryption key is lost by the organisation the data is rendered useless.Natural disaster, technical failure and accidental erasure of data can all affect cloud-based services in the same manner as an internal infrastructure.Also,malicious hackers may permanently delete cloud data to harm businesses as cloud data centres are very vulnerable to such attacks.

3. Account hijacking

It is the process by which an individual's or an organisation's account in the cloud is taken over or stolen by an attacker.Phishing, fraud, and software exploits still exist and cloud services add a new dimension to the threat because attackers can intrude on activities, manipulate transactions, and modify data. Attackers or hijackers may also use the cloud application to launch other attacks.During cloud account hijacking, an attacker typically uses a compromised email account or other credentials to impersonate the account owner. Because a huge amount of data stored in one

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

place is accessed on devices and resources are shared across many different users, the risks presented by cloud account hijacking are plentiful.

4. Regulatory compliance

A cloud service may have privacy or data protection laws and the specific regulations, such as HIPAA, the Sarbanes-Oxley or the EU Data Protection Directive, your business must comply with. Under these mandates, companies must know where their data is, who is able to access it, and how it is being protected .The cloud service must also be capable of providing you with all the necessary data, such as audit trails and logs, in the event of an audit or investigation. Storing data on a cloud service may mean your organization must comply with other regulations as your data may be physically stored in another country or even several different ones.When these regulations are violated, the organization might get into a state of non-compliance, which can have serious repercussions.

5. Data ownership and control

The move to the cloud will definitely lead to some loss of control of the organization's data as it is stored on the cloud provider's servers. Issues such as the geographic location of your data, specific backup processes and the steps taken to ensure your data is private and secure may no longer be in your control. This means that the service provider could have some degree of access to your data. In addition to privacy concerns relating to sensitive data, this may also impact your compliance controls and requirements.

6. Insider threats

This threat could be from anyone; the current or former employee, the system administrator, contractor or business partner.While attacks and misuse of data by your own employees may seem low-risk, the insider threat is very real. This can lead to the destruction of whole infrastructure, manipulation or misuse of important and sensitive data such as customer or financial information. Effective logging, monitoring, and auditing administrator activities can also be critical. Assigning incorrect access levels or neglecting to remove user access for former employees can also lead to users having access to information they should not have. Apart from users with malicious intention, the threat of accidental deletion or release of data also exists if they are not adequately trained in the use of the software.

7. Abuse of cloud services

Hackers or even authorized users may potentially attack and abuse cloud storage for illegal activities. This can include the storing and spread of copyrighted materials, sending spams, phishing emails, pirated software, hosting malicious content or viruses. This can occur when individuals directly attack the service or take over the cloud service's resources. Cloud resources can also be attacked directly through malware injection which involves hackers gaining access to the cloud and then running scripts containing hidden malicious code. Customers may not be directly affected by malicious actions, but cloud service abuse can still result in service availability issues and major data loss.

8. Denial of Service attacks

Distributed Denial of Service (DDoS) attacks have become more frequent, more sophisticated and larger in the recent years. Operating on a cloud-based service can increase the risk of being attacked as we share resources with all other users on the cloud, an attack on another tenant can result in our service being affected.With the amount of bandwidth consumed by large DDoS attacks, only very large cloud providers will be capable of withstanding the attack. DoS attacks consume large amounts of processing power, a bill the customer may ultimately have to pay. Though high volume DDoS attacks are very common, organizations should be aware of asymmetric, application-level DoS attacks, which mainly target Web server and database vulnerabilities.

These are the most common security threats that are encountered, while there are many more such as hacking interface and API's since the availability of cloud services depend on the security of API, parasitical forms of attack called APT's which infiltrate systems to establish a foothold, then stealthily exfiltrate data and intellectual property over an extended period of time,unauthorized access and insufficient due diligence.Cloud service providers share technology (infrastructure, platforms, and applications),along with which the dangers alsoget shared and if vulnerability arises in any of these layers, it affects everyone. This inevitably results in diminished trust by customers. With this information, IT teams can begin to take counter measures, enforce corporate data security, compliance, and governance policies to protect corporate data in the cloud. Therefore, the companies must balance the risks of cloud services with the clear benefits they bring.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

IV. CRYPTOGRAPHIC TECHNIQUES

Cryptography is the conversion of clear text into an unreadable form to ensure they can only be read by the intended recipient.Cryptographic techniques have become essential for security in cloud.Cryptography refers to the science of designing ciphers. A key is used for data encryption and decryption. It allows data to be stored securely and ensures security of data being shared in cloud. Encryption refers to the method of converting plain text to cipher text which can only be read by the owner of secret key.These processes come under the key management method.

A. *Key Management method*

A cryptographic key which is a string of bits is a core part of cryptographic algorithm. Encryption algorithm plays a vital role in protecting the data. Cryptography (E) makes data and messages secure by encrypting the plaintext (P) which is the input data and converts it into cipher text (C) and then performing decryption (D) which is reverting back to the plaintext called as decryption, using encryption keys(k1 and k2). This can be interpreted as Cipher text C = E {P, Key} and Plain text C= D {C, Key}.

The 2 major categories in cryptography algorithms are:

1. Symmetric key cryptography

It is one of the oldest and best known techniques. In symmetric key encryption the person who sends the data and the person who receives the data share a key. The key which they share is kept secret. The key can be a word, a number or a string of random letters. The same key is used for encryption and decryption. The 2 secret key encryption protocols are DES and AES.

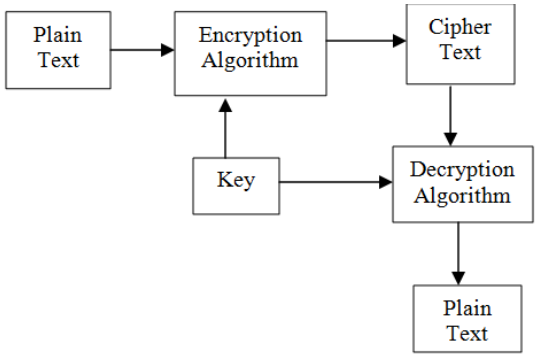

Figure 2: Symmetric key cryptography

2. Asymmetric key cryptography

In asymmetric key encryption(also known as public key cryptography), there are two keys. One key is used for encryption and another key is used for decryption. The secret keys are exchanged over the Internet or a large network. Asymmetric encryption is slower compared to symmetricencryption. The encryption key is known as thepublic key and the decryption key is known as the private key.The public and private keys are known as a key pair.A message that is encrypted using a public key can only be decrypted using a private key, and a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and is passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication. Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes RSA, DSA, Elliptic curve techniques etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

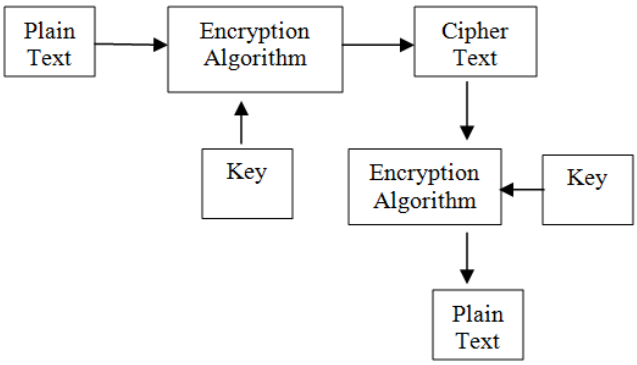

Figure 3: Asymmetric key Cryptography

B. *Description of the Algorithm:*

There are three different encryption algorithms namely; AES, DES and RSA.

1. Advanced Encryption Standard (AES)

Advanced Encryption Standard is a symmetric-key block cipher. It is a New encryption standard recommended by NIST to replace DES. AES is a non-Feistel cipher. AES encrypts data with block size of 128-bits. It uses 10, 12, or fourteen rounds. Depending on the number of rounds, the key size may be 128, 192, or 256 bits. AES Encryption is fast and flexible. It has been tested for many security applications.

2.Data Encryption Standard (DES)

DES is one of the most widely used cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46).In this, same key is used for encryption and decryption process.DES is 64 bits key size with 64 bits block size. At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit cipher text. At the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption.

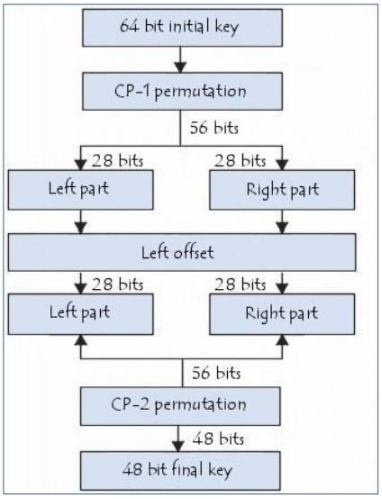

Fig. 4: DES Algorithm

3.Rivest-Shamir-Adleman(RSA)

RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman and is widely used public key algorithm. It is a homomorphic encryption for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

RSA algorithm involves these steps:
1. Key Generation
2. Encryption
3. Decryption

Step 1: Key Generation
1. Select two prime numbers, p and q.
2. Compute n = pqand φ(n)= (p − 1)(q − 1)
3. Select an integer a; gcd (φ(n),a)=1; 1 < a < φ(n)
4. Calculate b.
5. Return public key KU= {a,n} and private key KR={b,n}

Step 2: Encryption
Plaintext: M<n
With public key {a,n} , ciphertext is constructed as
$C=M^e \pmod n$

Step 3: Decryption
With ciphertextC, plaintext M is extracted by,
$M=C^d \pmod n$

Another approach to public-key cryptography is **Elliptic curve cryptography**.
Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller. An elliptic curve over a field K is a non-singular cubic curve in two variables, f(x,y) =0 with a rational point (which may also be a point at infinity). The field K is usually taken to be the complex numbers, reals, rationals, and algebraic extensions of rationals, p-adic numbers, or a finite field. Elliptic curves groups for cryptography are analysed with the underlying fields of Fp.

$$y^2=x^3+ax+b$$

(where p>3 is a prime) and F2m (a binary representation with 2m elements).
Every user has a public and a private key. A public key is used for encryption/signature verification and a private key is used for decryption or signature generation. Elliptic curves are used as an extension to other current cryptosystems. That is Elliptic Curve Diffie-Hellman Key Exchange and Elliptic Curve Digital Signature Algorithm.

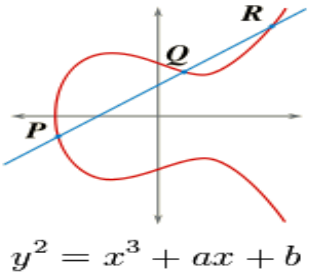

Fig 5: An elliptic curve

V. SIMULATION RESULTS

The graphical user interface (GUI) for simulating network data symmetric and Asymmetric Encryption techniques weredesigned, written and tested in Visual Basic 6.0 (VB 6.0) editor environment. Two Computer systems with different processing speeds were brought and the program ran on both of them to visualize the performance effect of different chosen encryption algorithms such as DES, AES and RSA. Different data block file sizes were encrypted and time taken to encrypt each captured and noted down.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

This implementation is thoroughly tested and optimized to give the maximum performance of the selected algorithmswhich are used in today's network data encryption.The Symmetric & Asymmetric encryption and decryption Performance in CPU 2.13GHz & 600MHz Systems are shown in the table below.

Data Block Size (bytes)	AES Time(s)	DES Time(s)	RSA Time(s)
72000	6	12	2
154000	8	20	4
203000	9	25	5
351000	12	40	8
476000	15	52	9.5
589000	17	64	11
718000	20	77	12
1222000	32	130	14
1715000	42	180	18
3156000	76	329	22

Table 5.1: Comparative execution time (in seconds) of Encryption algorithms in Computer CPU of 2.13 GHz

Data Block Size (bytes)	AES Time(s)	DES Time(s)	RSA Time(s)
72000	2	8	0.3
154000	4	16	1
203000	4	21	1.5
351000	8	36	3
476000	11	48	5
589000	13	60	5.5
718000	16	73	7
1222000	28	126	10
1715000	38	176	13
3156000	72	325	18

Table 5.2:Comparative execution time(in seconds) of Encryption algorithms in Computer CPU of 600MHz

The first set of experiments was conducted in computer CPU of 2.13 GHz processing speed. Different block data sizeswere selected and the algorithms tested in order to select the best out of the chosen algorithms. Table 5.1 shows the data block sizes and the output time response of each algorithm selected. The second set of experiments was conducted in Computer CPU of 600 MHz processing speed. The same block data sizes were used and the algorithms testedto select the best out of the chosen algorithms. Table 5.2 shows the data block sizes and the output time response of each algorithm after encryption.

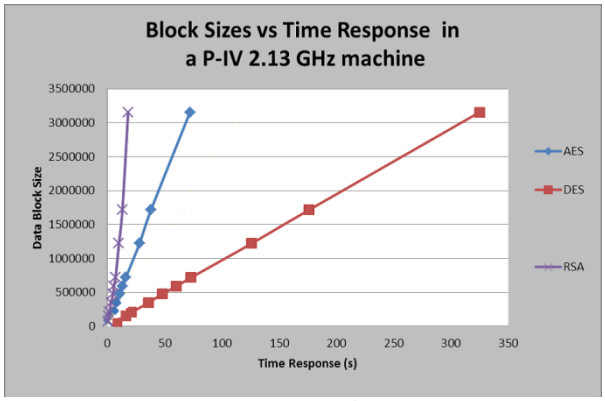

Fig 6.1: Block Sizes v/s Time Response of CPU 2.13 GHz machine

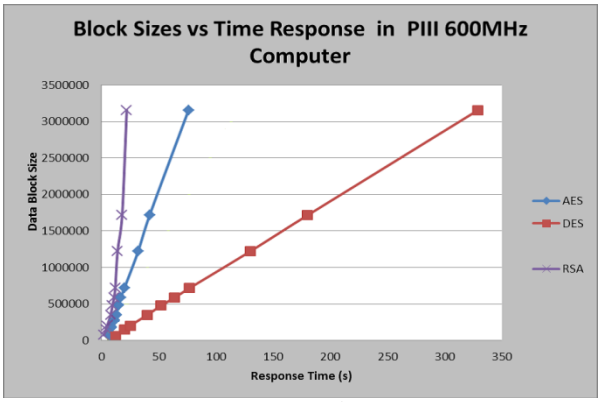

Fig 6.2: Block Sizes v/s Time Response of CPU 600 MHz machine

The data block sizes and time responses listed in table 5.1 and table 5.2 are plotted using Microsoft Excel. Thealgorithms behaviour shown on the graph results obtained are in figure 6.1 and figure 6.2. It is observed that RSA and AES have better performance over other algorithms in terms of throughput among all the symmetric encryption techniques. The result shows the superiority of RSA and AES algorithm over other algorithms in terms of the processing time. DES was seen to have worm hole in its security mechanism, AES, and RSA on the other hand, do not have any so far. These results have nothing to do with the other loads on the computer since each single experiment was conducted multiple times resulting in almost the same expected result.AES and RSA have the best performance among others. Both of them are known to have better encryption (i.e. stronger against data attacks) than the others.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

VI. CONCLUSION AND FUTURE WORK

With so many threats having been discussed in the paper, it is very clear as to why we need an encryption system. We are still very far from making cloud computing services completely secure and a trustworthy customer service. However, we have tried the best in making cloud computing safe and secure with the best possible solution. Though cryptography assures a certain level of safety, we can only hope that the future invention holds better solutions and can metamorphose the present technology to a better one.With the increasing demand and popularity of the cloud-based services, it is very necessary to protect the data and keep it safe.

REFERENCES

[1] https://www.ibm.com › IBM Cloud
[2] www.howstuffworks.com
[3] White Paper | Cloud-Based Security Technical Brief Series How to Evaluate the Data Security Capabilities of Cloud-Based Services
Cloud Computing Security Threats I Waterford Technologies
[4]Radhika Patwari1, SaritaChoudhary, "Security issues and Cryptographic techniques in Cloud Computing", International Journal of Innovative Computer Science & Engineering, Volume 2, Issue No.4, pp.3-4, September-October-2015.
[5] Cloud Security Risks Every Company Faces - Skyhigh Networks
[6]www.skyhighnetworks.com
[7] www.azure.microsoft.com
[8] www.infoworld.com/article/.
[9] https://support.microsoft.com/ description of symmetric and asymmetric algorithm
[10]PoojaBindlish, Pawan Kumar, "Study of RSA, DES and Cloud Computing", International Journal of Advanced Research in Computer Science, Volume 7, Issue No.3, pp.211, May-June 2016.
[11] Dr. PrernaMahajan&AbhishekSachdeva , "A Study of Encryption Algorithms AES, DES and RSA for Security ",Global Journal of Computer Science and Technology Network, Web & Security, Volume 13, Issue No.15, pp.15-19, Year 2013.
[12]Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security",International Journal of Computer Applications, Volume 67, Issue No.19, pp.35-37, April 2013.
[13] T.Ramaporkalai," Security Algorithms in Cloud Computing", International Journal of Computer Science Trends and Technology (IJCST) – Volume 5, Issue No.2, pp.501-502, Mar –Apr 2017.
[14] Homomorphic Cryptosystems ,EdlynTeske-Wilson University of Waterloo ,Ottawa, Canada
[15] XiaojiangDu,MohsenGuizani,Yang Xiao and Hsiao-Hwa Chen, "A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks",IEEE Transactions on wireless communications, Vol. 8, Issue No.3, March 2009.
[16] VeerrajuGampala, SrilakshmiInuganti,SatishMuppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE),Volume-2, Issue No.3, pp.139-140, July 2012.
[17] Wikipedia
[18] Ezeofor C. J., Ulasi A. G, "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems" , International Journal of Innovative Research in Science, Engineering and Technology ,Vol. 3, Issue 12, pp. 17797-17807, December 2014.

BIOGRAPHY

Varsha K is currently studying her Bachelor of Engineering in Computer Science and Engineering at St. Joseph Engineering College, Vamanjoor, Mangaluru, India. Her field of interest is Cloud Computing.

Rachel Mathias is currently studying her Bachelor of Engineering in Computer Science and Engineering at St. Joseph Engineering College, Vamanjoor, Mangaluru, India. Her areas of interest include Cloud Computing and Internet of Things.