IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 4, April 2019
ISSN (Online) 2348 – 7968
www.ijiset.com

Implementation of RSA Algorithm to Secure Data in Cloud Computing

Dr. Rajamohan Parthasarathy [1*] , Ms. Haw Wai Yee [2], Mr. Seow Soon Loong [3]
Dr. Leelavathi Rajamanickam [4], Ms. Preethy Ayyappan [5]

[1 *, 2, 3 & 4] School of Information Technology, SEGi University, Kota Damansara, Malaysia
[5] Faculty of Engineering and Built in Environment, SEGi University, Kota Damansara, Malaysia
* Corresponding author E-mail: prajamohan@segi.edu.my & Parthasarathy_rajamohan@yahoo.com

Abstract

Cloud computing stores the data and disseminated resources in the open environments. Even though the cloud computing is promising and efficient, there are many challenges for data security as there is no vicinity of the data for the cloud user. The security of cloud computing has always been an important aspect of quality of service from cloud service providers. Cloud computing is technical and social reality today, at the same time it is the emerging technology and security has become the main obstacle which is hampering the deployment of cloud environments. To ensure the security of data, we proposed a method for providing data storage and security in cloud using public key cryptosystem by implementing RSA algorithm. Further describes the security services includes key generation, encryption, decryption in virtual environment.

***Keywords**: Cloud Computing, Cloud security, Data Security, Encryption, Decryption, RSA Algorithm.*

1. Introduction

Cloud Computing Definition is that it is a shared pool of configurable computing resource (eg. networks, servers, storage, applications, and services) network on demand over the internet. Cloud computing literally, is the use of remote servers (usually accessible via the Internet) to process or store information. Access is usually using a Web browser. Save files on a server via the Internet is one example.

Securing data is always of vital importance and because of the critical nature of cloud computing and the large amounts of complex data it carries, the need is even more important. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services. As many companies move their data to the cloud the data undergoes many changes and there are many challenges to overcome. To be effective, cloud data security depends on more than simply applying appropriate data security procedures and countermeasures. Computer based security measures mostly capitalizes on user authorization and authentication.

This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.[1]-[3] The cloud computing model NIST defined has three service models and four deployment models. The three service models, also called SPI model, are: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS).

The four deployment models are: Private cloud, Community cloud, Public cloud and Hybrid cloud. Application data is stored in a manner that is device and location independent. Security of the cloud based applications and Data is the key concerns of the cloud computing. The principles of the security are the Confidentiality, Integrity and Availability.

Cloud security is a broad topic and any combination of policies, technologies, and controls to protect data, infrastructure and services from possible attacks.

Cloud Computing appears as a computational paradigm as well as a distributed architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [2][3].

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977.

In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it.

User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider, Cloud provider authenticates the user and delivers the data.

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data.

Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.[4]

1.1 Cloud computing service models

Cloud computing has been majorly divided into three broad service categories**:** Infrastructure as a Service (IAAS)**,** Platform as a Service (PAAS) and Software as a Service (SAAS) a shown in fig. 1: and detailed technical information as below.

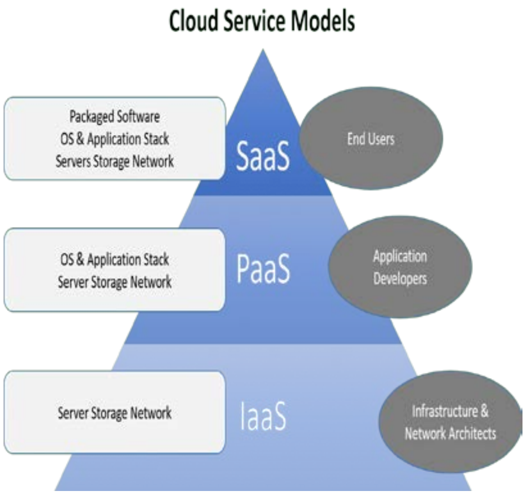


Fig. 1: Different Types of Cloud Computing Model

1.1.1 Infrastructure as a service (IaaS) is a form of cloud computing that provides virtualized computing resources over the internet. In a IAAS model, a third party provider hosts hardware, software, servers, storage and other infrastructure components on the behalf of its users. IAAS providers also host users' applications and handle tasks including system maintenance backup and resiliency planning. IAAS platforms offer highly scalable resources that can be adjusted on-demand which makes it a well-suited for workloads that are temporary, experimental or change unexpectedly. Other characteristics of IAAS environments include the automation of administrative tasks, dynamic scaling, desktop virtualization and policy based services. Other characteristics of IAAS include the automation of administrative tasks, dynamic scaling, desktop virtualization and policy based services [3]-[5]

1.1.2 Platform as a service (PaaS) is a cloud computing model that delivers applications over the internet. In a PAAS model, a cloud provider delivers hardware and software tolls, usually those needed for application development, to its users as a service. A PAAS provider hosts the hardware and software on its own infrastructure. As a result, PAAS frees users from having to install in-house hardware and software to develop or run a new application. A PAAS provider, however, supports all the underlying computing and software; users only need to login and start using the platform-usually through a Web browser interface. PAAS providers then charge for that access on a per-use basis or on monthly basis. Some of the main characteristics of PAAS are[3]-[5]:

- Scalability and auto-provisioning of the underlying infrastructure.
- Security and redundancy.
- Build and deployment tools for rapid application management and deployment.
- Integration with other infrastructure components such as web services, databases, and LDAP.
- Multi-tenancy, platform service that can be used by many concurrent users.
- Logging, reporting, and code instrumentation.
- Management interfaces and/or API.

1.1.3 Software as a service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SAAS has become increasingly prevalent delivery model as underlying technologies that support Web services and service- oriented architecture (SOA) mature and new development approaches, such as Ajax, become popular. SAAS is closely related to the ASP (Application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for SAAS namely the hosted application model and the software development model. Some of the core benefits of using SAAS model are [3]-[5]:

- Easier administration.
- automatic updates and patch management.
- compatibility: all users will have the same version of software.
- easier collaboration, for the same reason.
- global accessibility.

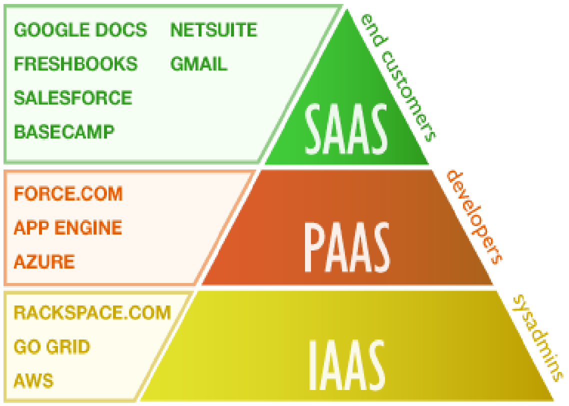


Fig. 2: Cloud Computing Model global view

1.2 Anything as a service (XaaS)

Some of the other service categories which are more commonly classified as below:

1.2.1 Storage as a service (SaaS) Storage as a Service is a business model in which a large company rents space in their storage infrastructure to a smaller company or individual. The economy of scale in the service provider's infrastructure theoretically allows them to provide storage much more cost effectively than most individuals or corporations can provide their own storage, when total cost of ownership is considered. Storage as a Service is generally seen as a good alternative for a small or mid- business that lacks the capital budget and/or technical personnel to implement and maintain their own storage infrastructure.

1.2.2 Communications as a service (CaaS) is an outsourced enterprise communications solution that can be leased from a single vendor. Such communications can include voice over IP (VoIP or Internet telephony), instant messaging (IM), collaboration and video conference applications using fixed and mobile devices. The CAAS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). CAAS allows businesses to selectively deploy communications devices and modes on a pay-as-you-go, as-needed basis.

1.2.3 Network as a service (NaaS) a framework that integrates current cloud computing offerings with direct, yet secure, client access to the network infrastructure. NAAS is a new cloud computing model in which the clients have access to additional computing resources collocated with switches and routers. NAAS can include flexible and extended Virtual Private Network (VPN), bandwidth on demand, custom routing, multicast protocols, security firewall, intrusion detection and prevention, Wide Area Network (WAN), content monitoring and filtering, and antivirus.

1.2.4 Monitoring as a service (MaaS) is a framework that facilitates the deployment of monitoring functionalities for various other services and applications within the cloud. The most common application for MAAS is online state monitoring, which continuously tracks certain states of applications, networks, systems, instances or any element that may be deployable within the cloud. MAAS makes it easier for users to deploy state monitoring at different levels of Cloud services.

1.3 Deployment models

In this section various Deployment Models are discussed:[11]-[12]

1.3.1 Private cloud: In this model cloud owner does not share their resources with any other organization. It is set up and maintained by an organization. Security can be very well implemented in this model.

1.3.2 Public cloud: In this cloud model the resources are accessed by general public. Everybody can access easily with this cloud so it is less secure model. Cost of this cloud is not expensive. This model requires a huge investment these are owned by large organizations such as Microsoft, Google or Amazon.

1.3.3 Community cloud: A cloud shares the two or more several organizations or companies for their requirements. Usually used in school or university campus.

1.3.4 Hybrid cloud: This type of cloud uses the one or more cloud model combinations for better use.

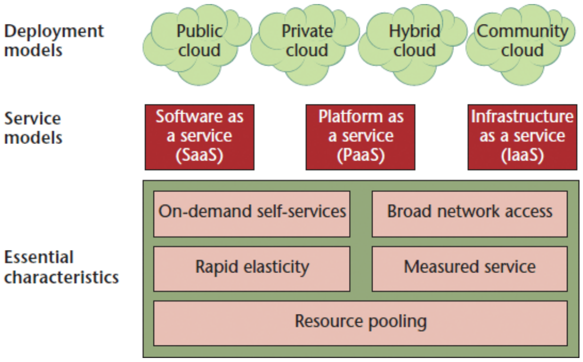


Fig. 3: Cloud computing service models and deployment model

2. Cloud data security issues

2.1 Privacy and confidentiality: Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential.[11]-[[12]

2.2 Data integrity: With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

For compliance purposes, it may be necessary to have exact records as to what data was placed in a public cloud, when it occurred, what virtual memories (VMs) and storage it resided on, and where it was processed. When such data integrity requirements exists, that the origin and custody of data or information must be maintained in order to prevent tampering or to prevent the exposure of data beyond the agreed territories.[11]

2.3 Data location and relocation: Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location. This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information. Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each other's resources.[11]-[12]

2.4 Data availability: Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.[12]

2.5 Storage, backup and recovery: When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers. [11]

In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.

3. Data security approaches

Hence Security of data has become a major concern. When data mobility is at a high level then the risks and issues increase many folds especially when data is transferred to another country with different regulatory framework.

High levels of data relocation have negative implications for data security and data protection as well as data availability.

Thus the main concern with reference to security of data residing in the Cloud is: how to ensure security of data that is at rest. Although, consumers know the location of data and there in no data mobility, there are questions relating to its security and confidentiality of it. No doubt the Cloud Computing area has become larger because of its broad network access and flexibility. But reliability in terms of a safe and secure environment for the personal data and info of the user is still required.

Financial savings, agility and elasticity, all enabled through cloud technology, are crucial in a fast paced business world. At the same time security incidents in the Cloud have made clear that this new promising technology comes with complexity and security and privacy challenges.

In Cloud computing Environment there are various security issues are occurs due sharing of resources it leads to a security problem.

Cloud computing as it comprises many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.

Therefore, security issues for many of these systems and technologies are pertinent to cloud computing. Cloud possesses the security problem in Data segregation, Data theft, unauthorized access, uncleared Owner and responsibility of Data Protection, Data Loss conditions.[11]-[13]

3.1 Data security framework

Security is the major concern to access the data in cloud. Security involves protecting data from being lost, destroyed or modified. [11]

This paper presents a survey on the cloud data security issues, Data security life cycle. To provide security for cloud data RSA Algorithm is used, these are all discussed in the further sections. [9]

3.1.1 Protection of data: Data can be protected from the outside user by creating the security keys such as private key.

3.1.2 Building blocks: The form of Mathematical and cryptographic principles server as the building blocks of the security.

3.1.3 Integrity of data: while uploading the data the user can verify the correctness of the integrity principles.

3.1.4 Accessing the data: Due to the Encryption and Decryption techniques data can be accessed securely.

3.1.5 Authentication: Authentication allows only authorised user to access Data in cloud.

3.2 Data security life cycle

The life cycle of the Data security includes the six phases as once data is created it can process through all the stages[11]-[13]

3.2.1 Create: Creation is the generation of the new digital data content, uploading and modifying the data.

3.2.2 Store: Storing is the act committing the digital data storage repository, and typically occurs nearly simultaneously with creation.

3.2.3 Use: Data is viewed, processed and retrieved actively.

3.2.4 Share: Data is exchanged between the users, customers, and partners of the respective cloud.

3.2.5 Archive: Data leaves active use and enters long-term storage.

3.2.6 Destroy: Data is destroyed permanently using the physically or digital name.

Create
Store
Use
Share
Archive
Destroy

Fig.4: The life cycle of Data security

4. The proposed methodology

The area of cryptography and cryptanalysis together are known as cryptology [8]. Cryptanalysis used many encryption and decryption techniques such as Caeser cipher, Monoalphabetic cipher, Play fair cipher, Hill Cipher. These techniques possess the Brute Force Attack means the attacker tries every possible key to get the original text to avoid this problem public key cryptography used.

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977.

In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it.[8][9]

4.1 RSA algorithm: is the public key cryptography, in which both public and the private keys are used to secure data in cloud. The development of the Public key cryptography is greatest and perhaps it provides a radical departure. It is also known as the Asymmetric algorithm due to the use of two key along with secret key. In this scheme the plain text and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits.[14]-[15]

User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider, Cloud provider authenticates the user and delivers the data.[7]-[9]

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

4.2 RSA algorithm involves three steps:

1. Key Generation

2. Encryption

3. Decryption

4.2.1 Key generation: Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.[14]

4.2.1.1 Key generation algorithm

Steps:

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be 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. Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of 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 multiplicate inverse of e mod Ø(n).

6. d is kept as Private-Key component, so that
d * e = 1 mod Ø(n).

7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).

8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n). [7][8][9], [14][15]

4.2.1.2 Encryption algorithm:

Encryption is the process of converting original plain text (data) into cipher text (data).[7]-[9], [14][15]

Steps:

1. Cloud service provider should give or transmit the Public- Key (n, e) to the user who want 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 $C = m^e$ (mod n).

4. This cipher text or encrypted data is now stored with the Cloud service provider.

4.2.1.3 Decryption algorithm:

Decryption is the process of converting the cipher text(data) to the original plain text(data).[7]-[9], [14]

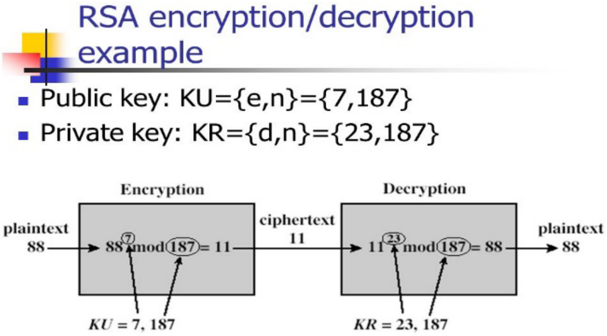
Steps:

1. The cloud user requests the Cloud service provider for the data.

2. Cloud service provider verify's the authenticity of the user and gives the encrypted data i.e, C.

3. The Cloud user then decrypts the data by computing, $m = C^d$ (mod n).

4. Once m is obtained, the user can get back the original data by reversing the padding scheme.[15]



RSA encryption/decryption example

- Public key: KU={e,n}={7,187}
- Private key: KR={d,n}={23,187}

Fig. 5- RSA Encryption/Decryption Example.

5. Experimental results and analysis

In this section, we are taking some sample data end implementing RSA algorithm over it.

5.1 Key generation part:

1. We have chosen two distinct prime numbers a=61 and b=53.

2. Compute n=a*b, thus n=61*53 = 3233.

3. Compute Euler's totient function, Ø(n)=(a-1)*(b-1), Thus Ø(n)=(61-1)*(53-1) = 60*52 = 3120.

4. Chose any integer e, such that 1 < e < 3120 that is coprime to 3120. Here, we chose e=17.

5. Compute d , $d = e^{-1}$(mod Ø(n)),

thus $d=17^{-1}$(mod 3120) = 2753.

6. Thus the Public-Key is (e, n) = (17, 3233) and the Private- Key is (d, n) = (2753, 3233).

This Private-Key is kept secret and it is known only to the user.

5.2 Encryption part:

1. The Public-Key (17, 3233) is given by the Cloud service provider to the user who wish to store the data.

2. Let us consider that the user mapped the data to an integer m=65.

3. Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and the user.

$C = 65^{17}$(mod 3233) = 2790.

4. This encrypted data i.e, cipher text is now stored by the Cloud service provider.

5.3 Decryption part:

1. When the user requests for the data, Cloud service provider will authenticate the user and delivers the encrypted data (If the user is valid).

2. The cloud user then decrypts the data by computing,

$m = C^d$(mod n) = 2790^{2753}(mod 3233) = 65.

3. Once the m value is obtained, user will get back the original data.

6. Conclusion

The flexibility of the cloud is allocation of the resources on demand. The RSA Algorithm provides the high secure and high potential Data Encryption methodology. It is highly secure than all other Encryption techniques. Cloud Computing is still a new and evolving paradigm where computing is regarded as on-demand service. Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he/she captures the data also, he/she can't decrypt it and get back the original data from it. Hence forth, data security is provided by implementing RSA algorithm. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography.

References:

[1] Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2, 2011, pp: 1836-1840, .

[2] Wiiliam Stallings, "Cryptography and Network Security: principle and practices" by sixth edition published by Pearson Education Inc@2014

[3] Anshuman Biswasr, Shikharesh Majumdar, Biswajit Nandy, Ali El-Haraki, "A hybrid auto-scaling technique for clouds processing applications with service level agreements", Biswas et al. Journal of Cloud Computing: Advances, Systems and Applications (2017) 6:29 DOI 10.1186/s13677-017-0100-5, pp 1-22

[4] Devi T, "Data Security Frameworks In Cloud", School of Computing Sciences and Engineering International Conference on Science, Engineering and Management Research (ICSEMR 2014) 978-1-4799-7613-3/14/ ©2014 IEEE.

[5] M.Sasikala , Dr. V. Anuratha, "Analysis Of Security Algorithms In Cloud", International Journal Of Advanced Research In Science And Engineering, Volume No. 6, Issue No. 12, Year 2017, pp. 631-641.

[6] Coppersmith, Don (1997). "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities" (PDF). Journal of Cryptology. 10 (4): 233–260. doi:10.1007/s001459900030.

[7] Wiener, Michael J. (May 1990). "Cryptanalysis of short RSA secret exponents" (PDF). Information Theory, IEEE Transactions on. **36** (3): 553–558. doi:10.1109/18.54902.

[8] Johnson, J.; Kaliski, B. (Feb 2003). "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1". www.ietf.org. Network Working Group. *Retrieved 9 March 2016.*

[9] "RSA Security Releases RSA Encryption Algorithm into Public Domain". Archived from *the original* on June 21, 2007. *Retrieved 2010-03-03.*

[10] Matus Nemec, Marek Sys, Petr Svenda, Dusan Klinec,Vashek Matyas, "The Return of Coppersmith's Attack:" Practical Factorization of Widely Used RSA Moduli, , November 2017.

[11] Birendra Goswani, Dr.S.N.Singh, "Enhancing Security in Cloud computing using Public Key Cryptography with Matrices", International Journal of Engineering Research and Applications, Vol 2, Issue 4, 339-344, July-Aug 2012.

[12] V. Sandhya, "A Study on Various Security Methods in Cloud Computing", International Journal of Advanced Research in Computer Science, Volume 2, No.6, Nov-Dec 2011

[13] G. Jai Arul Jose, C. Sanjeev, Dr. C. Suyambulingom, "Implementation of Data Security in Cloud Computing", International Journal of P2P Network Trends and Technology, Vol 1, Issue 1, 2011

[14] Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International Journal of Computer Science and Information Technology, Vol. 2(3), 2012, pp: 242-249.

[15]. Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance Cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 1, Jan 2012.