HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 8, March 2014
e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-499-4

A Survey of Cryptographic based Security Algorithms for Cloud Computing

***Mayank Patwal*[*] *and Tanushri Mittal*[†]**
mayank.patwal@gmail.com

Abstract

Cloud computing is the outsourcing of IT communications by the use of the Internet and maintaining own hardware and software environment. Cloud computing facilitates computing assets on demand by the use of a service provider. It is there whenever you need it, as much as you need, and you pay as you go and only for what you use. Security is a prim concern in the use of cloud computing. In this paper, we have presented a survey of cryptographic based security algorithms for cloud computing.

Keywords

Cloud Computing, Security Issues, Cryptography, Security Algorithms.

[*] M.Tech Student, Department of Computer Science & Engineering, Graphic Era University, Dehradun, India

[†] Assistant Professor, Department of Computer Science & Engineering, Graphic Era University, Dehradun, India. Email: tanushrimittal.86@gmail.com

Introduction

Cloud computing is the outsourcing of IT communications by the use of the Internet and maintaining own hardware and software environment. Cloud computing facilitates computing assets (processor compute time and data storage) on demand by the use of a service provider. Comparisons of cloud services are made by their nature and utilize services such as gas or electricity. It is there whenever you need it, as much as you need, and you pay as you go and only for what you use.

Now a day's Security of data has become a big distress. High levels of data repositioning have off-putting implications for data security and data shield as well as data availability. Thus the main worry regarding security of data residing in the Cloud is: how to make sure the security of data which is at rest. Although, consumers know the dimensions and location of web data high in no data mobility, you can find questions associated with its security and confidentiality of the USB ports. To be sure the Cloud Computing area happens to be larger to its broad network access and flexibility. But reliability regarding a secure and secure environment to the personal data and info on the user is still required.

NIST definition of cloud computing *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

Cloud computing is a form of information technology which is being used where lesser investment in efficient software is needed. Cloud computing consists of Access to applications and services is enabled over the network and it also require only access to internet connection. Possibly one can get access of the cloud with the use of an ordinary client simply anywhere and any-time and one needs a certain information facility, without any special software. Cloud computing also facilitates the clients for immediate access to pre-set common but valuable information resources (as access to the network, hardware, storage capacities, software, and special information services) that are eagerly available without a wide agreement making process.

Here we also can describe cloud computing by four fundamental characteristics, three service models and four deployment models.

Fundamental Characteristics of Cloud Computing

1. `Self-service on Requirement`: The user possibly will make a decision on the use of computing amenities such as server time and network storage alone, based on of their current needs, with no excess communication with dissimilar service providers.

2. `Broad Network Access`: Computing amenities possibly be accessed over the network through the use of standardized mechanism that hold up different clients, like mobile phones, tablets, laptops and work stations.

3. `Combining of Computing Resources`: Besides of classical virtualization, cloud computing uses in addition the capabilities of automation of services and multi-tenancy of users at common information resources. Common use of the same technological resources is the central feature of cloud computing. Before slideshow cloud provider had to establish divided infrastructures for different users, however an upswing of multi-tenancy mechanisms you are able to provide homogeneous configuration, uniform control in the services, upgrading and simpler disaster recovery processes and restoring from the data. Another essential feature is closely connected - the info are certainly not necessarily linked with a precisely defined strategic location anymore, simply because they can simultaneously be located in several data centres, all over the world.

4. `High Elasticity`: The consumer may easily increase or decrease the computing capacities afforded using the current requirements. The capacities are unlimited for the user.

Service Models of Cloud Computing

Cloud computing employs a service-driven business model. In other words, hardware and platform-level resources are provided as services on an on-demand basis. Conceptually, clouds offer services that can be grouped into three categories: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

1. `Infrastructure as a Service`: IaaS provide on-demand provisioning of infrastructural resources and does not manage or control the infrastructure and only manage and control the storage, application and selected network components. The cloud owner who offers IaaS is called an IaaS provider. Examples: Amazon EC2 .

2. `Platform as a Service`: PaaS providing software development frameworks and platform layer resources including operating system support. In PaaS user controls their application and does not manage servers and storage. Examples: Google App Engine,Microsoft Windows Azure etc.

3. `Software as a Service`: SaaS providing on demand applications all over the Internet. In SaaS user does not control or manage the servers, storage, network and application. Examples: Rack space etc.

Deployment Models of Cloud Computing

The deployment models of cloud computing are the following:

1. `Public Clouds` are publicly accessible and in this types of clouds are managed by third party.

2. `Private Clouds` are only accessible in private network. Private cloud infrastructure made available only a specific member and managed by organization itself or third party service provider.

3. `Community Clouds` are only accessible to a few numbers of clients with known features.

4. `Hybrid Clouds` are composition of two or more clouds.

The cloud service providers submit to a number of advantages cloud computing offers: from nominal costs because of the short of investment in, for example, hardware, to higher and quicker adaptability to the requirements of the client (you can obtain additional capacities when desired), and the suspected lower costs of repairs, support and other services attached to the ICT human resources. In some models, often all you require is access to the internet, a web browser.

Advantages and Disadvantages of Cloud Computing

The following are the common advantages of cloud computing:

1. `Lesser Cost`: Pay as you go, negligible hardware investments or software licenses.

2. `Added Performance`: on demand processing time, even HPC, if required.

3. `Fewer Maintenance`: somebody else manages the servers along with core software.

4. `Extra Security`: easily repair, enforcement of policies, centralized data.
5. `Extra Wide Storage Capacity`: Use it when you require it.

The most cited possible disadvantages of cloud computing are:

1. Dependency on Internet connectivity: Requires a regular connection.
2. Loss of control: The trouble of someone else hosting hardware, software and data, which out come in security concerns.
3. Unpredictable cost: Pay as you go means that the price of computing will be differ every month.

Data Security in Cloud Computing

Major concern is security of data. Data relocation on high level has negative implications for data safety and data security as well as data availability. Thus the main apprehension with reference to safety of data residing in the Cloud is: at the rest how to safe security .Although, customers know the location of data and there in no data mobility, there are question relating to its security and secrecy of it. No confusion the Cloud Computing area has become bigger because of its wide network access and flexibility. But we can also rely in terms of a safe and secure atmosphere for the personal data and info of the user is being required.

Data Security Issues in Cloud Computing

1. `Privacy and Confidentiality`: Once the client show data to the cloud there should be some security that access to that data will only be incomplete to the authorized access. Inappropriate access to client sensitive data by cloud staff is another risk that can create potential threat to cloud data. The client is being provided assurance and proper practices and safe policies and procedures should be in place to guarantee the cloud users of the data safety. The cloud seeker must be assured that data propagate on the cloud will be confidential.
2. `Data Integrity`: With getting the security of data, cloud service providers should apply mechanisms to ensure data truthfulness and be able to tell what happened to a definite data set and at what point. The client should be aware by the data provider the origin and the integrity mechanisms put in place

3. `Data Location and Relocation`: Cloud computing offers a high amount of data mobility. Consumers do not always know location of their data. However, when an venture has some sensitive data that's reserved over a storage device in the Cloud, they will often keep asking the career than it. They will also aspiration to specify a chosen location (e.g. data being trapped in India). This, then, needs a contractual agreement, between your Cloud provider and also the consumer that data should live in a certain location or reside on a given known server. Also, cloud providers should take accountability to guarantee the security of systems (including data) and gives robust certification to protect customer's information.

4. `Another concern` is the progress of web data in one location completely to another. Data is initially stored at a suitable location decide from the Cloud provider. However, it is moved derived from one of destination to another. Cloud providers have contracts jointly and in addition they use each other's resources.

5. `Data Availability`: Customer info is normally saved in chunk on different servers often residing in different locations or even in different Clouds. In such cases, data availability becomes a major legitimate issue because use of un-interruptible and seamless provision becomes relatively difficult.

6. `Storage, Backup and Recovery`: If you choose to maneuver crucial computer data for the cloud the cloud provider make certain adequate data resilience storage systems. by the side of a minimum they need to be able to present RAID (Redundant Array of Independent Disks) storage systems while most cloud providers will store the details in many copies some independent servers. In adding to that, most cloud providers have to be able to provide options on backup services which are definitely important for those businesses that jog cloud based applications so that in the occasion of a grim hardware failure and can roll back to an earlier state.

Security Advantages in Cloud Environment

Many large system are operated by current cloud service. They have complicated processes and specialization for maintaining their systems, which tiny enterprises may not have access to. As a result many direct and indirect security advantages for the cloud users. Here we show some of the key protection advantages of a cloud computing atmosphere.

1. `Data Centralization`: In a cloud atmosphere, the service provider takes care of storage issues and small business don't spend a extra money on storage devices. Also, cloud based storage provides a technique to physical centralize the data more rapidly and potentially cheaper and useful for small businesses, which cannot spend money on security professionals to monitor the data.

2. `Incident Response`: IaaS providers can offered a dedicated forensic server which they can use at the moment basis. Every time a security contravention occurs, the server could be brought online. In some investigation cases, backup with the environment can be simply made and hang onto the cloud without having affecting the traditional span of business.

3. `Forensic Image Verification Time`: Some cloud storage implementations picture a cryptographic check sum or hash. For example, Amazon S3 generates MD5 (Message-Digest algorithm 5) hash without human intervention when you store an object. Therefore in theory, the need to produce time consuming MD5 checksums with external tools is eliminated.

4. `Logging`: In a usual computing paradigm generally, logging is repeatedly an afterthought. In common, insufficient disk space is allocated that makes logging either non-existent or minimal. However, in a cloud, storage require for standard logs is automatically solved.

Security Disadvantages in Cloud Environment

In spite of security advantages, cloud computing paradigm also shows some key security challenges. Here we look at some key security challenges.

1. `Data Location`: In general, cloud users are not aware of the exact position of the data center and also they do not have any power over the physical access mechanisms to that data. Most famous cloud service providers have datacenters around the globe. Some service providers also take benefit of their global data centers. Though, in some cases applications and data may be stored in countries, which can judiciary concerns. For example, if the user data is stored in A country then service providers will be subjected to the security requirements and legal obligations of A country. This may also take place that a user does not keep the information of these issues.

2. `Investigation`: Investigating an illegitimate movement may not be possible in cloud environments. These investigations are hard by Cloud

services because data for multiple clients may be co-located and may also be increase across multiple data centers. Users have little information about the network topology of the underlying environment. Service provider may also enforce restrictions on the network security of the service users.

3. `Data Segregation`: Data in the cloud is usually in a shared environment together with data from other clients. Encryption cannot be understood as the single solution for data separation problems. In some situations, customers would not like to encrypt data because there can be a case when encryption accident can demolish the data.

4. `Long-term Viability`: When changing business situation as mergers and acquisition service providers must ensure the data safety. Customers must ensure data accessibility in these situations. Service provider also makes sure data security in harmful business conditions like prolonged outage etc.

5. `Compromised Servers`: In a cloud computing situation, users do not have a choice of using physical acquisition toolkit. In that situation, where a server is compromised; they need to close their servers down till they get a earlier backup of the data. This will more cause availability concerns.

6. `Regulatory Compliance`: External audits and security certification are subjected by traditional service provide. If a cloud service provider does not hold to these security audits, then it leads to a noticeable decrease in customer trust.

7. `Recovery`: Cloud service providers make sure the data security in ordinary and man-made disasters. Generally, data is virtual across multiple sites. However, in the case of any such unnecessary event, provider must do a comprehensive and quick restoration.

Literature Survey

Rahul Bhatnagar et al. (2013) in **Security in Cloud Computing** [16] have proposed an analysis of technical component and some research in threats for cloud computing Users and threats for cloud service provider then provide many security topics related for cloud security standardization(i.e. Storage Security, Data and Privacy Protection, Virtualization Security, Security Architecture/Model and Framework, Security Management and Audit Technology).

Shivashankar ragi (2011) within a research thesis **Security Approaches for Protecting Data in Cloud Computing** [19] have described the security threats and identify the safety approaches for security in cloud computing and measured the protection challenges and security methods of cloud computing and lastly identified from research methods quite a few challenges and techniques used now study plus in future research work in Cloud Computing.

Sanjana sharma et al. (2012) in **Security in Cloud Computing** [17] have described the briefly details of cloud computing and type of services and security issues and some challenges for data security in cloud environment and investigate the several approaches for security in cloud computing and finally provide a reliable security in cloud computing for future work.

Odunayo O. Owopetu (2013) in a research thesis **Private Cloud Implementation and Security** [18] have provide the easiest way to developed a private cloud for an enterprises using eucalyptus and possible ways of effectively securing it. Thesis report is divided two part: In first part basic information about cloud, cloud deployment model and cloud architecture. In second part describe the implementing private cloud using the Eucalyptus.

Uma Somani et al. (2010) in **Implementing the Digital Signature with RSA Encryption Algorithm to Boost the Data Security of Cloud in Cloud Computing** [20] have described the cloud storage methodology and proposed algorithm and Implementing the RSA algorithm through Digital Signature. and proposed the gradually process consumed in Digital Signature with RSA algorithm. If these implementing algorithms are combined in other encryption techniques(i.e. DES,AES etc) then its became stronger and secure for cloud computing.

Sanjana Dahal (2012) in a research thesis **Security Architecture for Cloud Computing Platform** [1] have focused on derive the secure and generic architecture for cloud computing platform without knowing its services and models. In this research paper most important object is delivering seamless access control,identity,authentication and service oriented architecture service to end user.

Sadia Marium et al. (2012) in **Implementation of Eap with RSA for Enhancing the Security of Cloud Computing** [2] have focused on service provider side security. In cloud computing data are protect from the unauthorized person, denial of services and misuse. In this paper highlights the cloud security policies and privacy issues and proposed the extensible authentication protocol for authentication with RSA algorithm.

Rodrigo N. Calheiros et al. (2011) in **CloudSim: A Toolkit for Modelling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms** [3] evaluating the performance of cloud policies, resource performance and application work load is very difficult to achieve then he proposed CloudSim an extensible simulation toolkit whose enable models and reproduction of Cloud computing systems.

Shucheng Yu et al. (2010) in **Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing** [4] have describe cryptographic method provide better confidentiality and security of sensitive data outsourced by user shared on cloud server. To achieve securing and secure access control, we may use uniquely combining techniques of attributes based encryption (ABE), proxy re-encryption and lazy re-encryption.

Ramgovind S et al. (2010) in **The Management of Security in Cloud Computing** [5] have described and highlight the overall security concern whose managed to realize the whole cloud computing and discuss about the Gartner's list on the cloud security issues. In this paper highlight each of security requirements of cloud computing and telling about the how to manage the cloud computing security.

Qian Wang et al. (2011) in **Enabling Public Audit Ability and Data Dynamics for Storage Security in Cloud Computing** [6] have described security of data stored in cloud is a achieved by allowing a third party auditor(TPA), which verify the integrity of the dynamic data stored in cloud. TPA can perform multiple auditing task simultaneously. Each operation on data is attached with authentication tag. Here we use Merely hash tree construction for blog tag authentication.

P. Syam Kumar et al. (2010) in **Ensuring Data Storage Security in Cloud Computing using Sobol Sequence** [12] have focus on ensuring data storage which is important of quality of services and proposed to address data storage security in cloud computing which is effective and flexible distribution verification protocol and describe the Sobol sequence using to check integrity of erasure coded data in cloud data storage.

Farzad Sabahi (2011) in **Virtualization-Level Security in Cloud Comput-**

ing [7] have summarize the cloud computing issues (i.e. Reliacbility, Availability and Security) and gives the available solution for cloud issues. In this paper summarize and telling step by step virtualization level of cloud computing security.

Jen-Shang Wang et al. (2011) in **How to Manage Information Security in Cloud Computing** [11] have described the key success factor whose determine the management information security and evaluating the hierarchical structure for key success factor. Based on these(external dimension, internal dimension, technology dimension and execution dimension) have analysis and categorization using fuzzy analytic hierarchy process.

Mohammed A. Alzain et al. (2011) in **MCDB: using Multi-Clouds to ensure security in Cloud Computing** [9] have proposed a multi clouds database model and present the architecture of multi cloud database model and describe the layers and components.

Huaglory Tianfield (2012) in **Security issues in Cloud Computing** [10] have discussed the taxonomy for security issues and discuss about all the distinctive characteristic of cloud(i.e multi-tenancy, elasticity etc) and third party control, then analyse the cloud security requirements(i.e. confidentiality, integrity and availability) and finally summarize the security issues in cloud computing based on the cloud security architecture.

Nelson Gonzalez et al. (2011) in **A Quantitative Analysis of Current Security Concerns and Solution for Cloud Computing** [8] have identify the main security problems and gives the solution in cloud computing. In this paper propose the taxonomy architecture of security and privacy in cloud computing and divided the security problem and security solution with grouped map.

Mr. Prashant Rewagad et al. (2013) in **Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing** [13] have modified AES encryption algorithm with digital signature and diffie Hellman key exchange to protect the data stored in cloud computing. In this paper described the three-way mechanism for protecting the data in cloud computing.

Hamid Banirostam et al. (2013) in **A Trust based Approach for Increasing Security in Cloud Computing Infrastructure** [14] have proposed Trusted Cloud Computing infrastructure whose inspired by Trusted Cloud Computing

Platform and proposed User Trusted Entity (UTE) that manage of IaaS system and UTE allows users to authenticate IaaS server. UTE are resolve the challenge of confidentiality, accuracy and integrity.

Mohammed A. AlZain et al. in **A New Approach Using Redundancy Technique to Improve Security in Cloud Computing** [15] have proposed the security to adopt data confidentiality, integrity and availability. He proposed a new model called multi-clouds database. This model uses multi cloud service provider, like Amazon cloud service. In this model Shamir's secret sharing approach is also proposed. In addition a Triple Model Redundancy techniques (TMR) and sequential method to improve the cloud computing systems security and reliability.

Some of the Existing Algorithms in Cloud Security

RSA Algorithm

RSA algorithm is public key encryption. This algorithm is brought to life by Ron Rivest, Adi Shamir and Len Adelman in 1977. It is hottest asymmetric key cryptographic algorithm. It may well used to provide secrecy. Therein algorithm uses the top number to come up with people key and key depending on mathematical fact and multiplying huge numbers together. It uses the block size data during which plain-text and cipher text are integers between 0and n for a lot of n values. Size n is known as 1024 bits. The real challenge in the case of RSA algorithm would be the selection and generation of the public and private key. Within this two different keys can be used encryption and decryption. As sender knows about the encryption key and receiver knows about the decryption key, the way we can generate encryption and decryption get into RSA. the whole process are made in below:

Choose large prime numbers p and q such that p$\doteqdot$ q.
Compute $n = p * q$
Compute $\phi(pq) = (p - 1) * (q - 1)$
Choose the public key e such that gcd $(\phi(n), e) = 1; 1 < e < \phi(n)$
Select the private key d such that $d * e$ mod $\phi(n) = 1$.
So in RSA algorithm encryption and decryption are performed as:
Encryption: Calculate cipher text C from plain-text message M such that: $C = M^e$ mod n
Decryption: $M = C^d$ mod n

DES Algorithm

Data Encryption Standard (DES) also known as as the Data Encryption Algorithm. DES algorithm provides improvement over the RSA algorithm. The speeds of DES encryption can be several M per second, It can be well suited for encrypted numerous message. RSA algorithm will be based upon the issue of factoring, and it is computing velocity is slower than DES,RSA algorithm is merely well suited for encrypting a tiny bit of data, The RSA encrypt the data essentially 117 bytes of once.

DES is really a block cipher. It encrypts the data in block height and width of 64 bits each. That's 64 bits are plain text goes as the input to DES, which produces 64 items of cipher text. Same key and algorithm can be used as encryption and decryption.DES uses 56 bit key but initial key is made up of 64 bits. Key is 56 items of 8, 16,24,32,40,48,56,64 are discarded (these bits may be used for parity checking to make certain the true secret doesn't contain any errors).Two fundamental features of cryptography Diffusion (Substitution) and Confusion (Permutation) rounds. In each round key and data bits are shifted, permuted, XORed and sent through, 8 round 64 bit plain-text is handed to initial permutation (IP).Then IP generates two halves left plain-text (LPT)and right plain-text (RPT).Each LPT and RPT goes through 16 rounds. At the last LPT and RPT are rejoined. Decryption is same process perform rounds in reverse order.

AES Algorithm

AES algorithm is symmetric and parallel structure. AES is gives the implementation of the algorithm many flexibility. AES is usually compares well against cryptanalsis attacks. AES algorithm is is useful with modern processor and deal with smart cards. AES key block size and length size from 128 and 256 bits inside the step of 32 bits. AES necessitates that the plain text block size has to be 182 bits and key size should be 128,192 or 256 bits.In generally two version of AES are widely-used: 128 bit plain text block joined with 128 bit key block and 128 bit plain text block with 256 bit key block.

Digital Signature

Cryptographic digital signatures use public key algorithms to deliver data integrity. When you sign data which has a digital signature, other people can verify the signature, and may prove that the data descends from you and hasn't been altered after you signed it.

In public key cryptography, anything 'A' encrypts with 'B"s public key may be decrypted by 'B' while using corresponding private key. 'A' may encrypt a message along with her private key, meaning that 'B' can decrypt it with 'A"s public key. Because public key is, because the name suggests, publicly available, this is not good idea if 'A' wishes to keep that message a secret. Eve could also simply get a copy of A's public key thereby also decrypt the material.

But because 'A' keeps her private key to herself, 'B' recognizes that only 'A' may have encrypted this message. 'B' is now sure that this message was compiled by 'A'. A signature on a paper message may serve as proof that it message was authored by the person who signed it. Encrypting having a private key thus might be thought to be an the same as placing one's signature within the message. For this reason this is what's called setting up a digital signature to the message.

References

[1] Sanjana Dahal, Security Architecture for Cloud Computing Platform, Master of Science Thesis Stockholm, KTH Industrial Engineering and Management, TRITA-ICT-EX-2012:291, Sweden, 2012.

[2] Sadia Marium, Qamar Nazir, Aftab Ahmed, Saira hthasham Mirza Aamir Mehmood, Implementation of Eap with RSA for Enhancing The Security of Cloud Computing, International Journal of Basic and Applied Sciences, 177-183, 2012.

[3] Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, Cesar A. F. De Rose and Rajkumar Buyya, CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Wiley Online Library, DOI: 10.1002/spe.995, 2011.

[4] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, 978-1-4244-5837-0/10,IEEE, 2010.

[5] Ramgovind S, Eloff MM, Smith E, The Management of Security in Cloud Computing, 978-1-4244-5495-2/10, IEEE,2010.

[6] Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, Kui Ren, Member, IEEE,Wenjing Lou, Senior Member, IEEE, and Jin

Li, Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011.

[7] Farzad Sabahi, Virtualization-Level Security in Cloud Computing, Faculty of Computer Engineering Azad University Iran,978-1-61284-486-2/11,IEEE, 2011.

[8] Nelson Gonzalez, Charles Miers, Fernando Redgolo, Tereza Carvalho, Marcos Simplicio, Mats Naslund and Makan Pourzandi, A quantitative analysis of current security concerns and solutions for cloud computing, 978-0-7695-4622-3/11, IEEE, 2011.

[9] Mohammed A. AlZain, Ben Soh and Eric Pardede, MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing, 978-0-7695-4612-4/11, IEEE, 2011.

[10] Huaglory Tianfield, Security Issues In Cloud Computing, School of Engineering and Built Environment Glasgow Caledonian University, United Kingdom, 978-1-4673-1714-6/12, IEEE, 2012.

[11] Jen-Sheng Wang, Che-Hung Liu, Grace TR Lin, How to Manage Information Security in Cloud Computing, 978-1-4577-0653-0/11, IEEE, 2011.

[12] P. Syam Kumar, R. Subramanian and D. Thamizh Selvam, Ensuring Data Storage Security in Cloud Computing using Sobol Sequence, 978-1-4244-7674-9/10., IEEE, 2010.

[13] Mr. Prashant Rewagad, Ms.Yogita Pawar, Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing, 978-0-7695-4958-3/13, IEEE, 2013.

[14] Hamid Banirostam, Alireza Hedayati, A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure, 978-0-7695-4994-1/13, IEEE, 2013.

[15] Mohammed A. AlZain, Ben Soh and Eric Pardede, A New Approach Using Redundancy Technique to Improve Security in Cloud Computing, Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia.

[16] Rahul Bhatnagar, Suyash Raizada, Pramod Saxena, SECURITY IN CLOUD COMPUTING,International Journal For Technological Research In Engineering, ISSN (Online) : 2347 4718, December - 2013.

[17] Sanjana Sharma, Sonika Soni, Swati Sengar, Security in Cloud Computing, National Conference on Security Issues in Network Technologies, 2012.

[18] Odunayo O. Owopetu, Private Cloud Implementation and Security, Bachelor's Thesis (UAS) , School of Computing Blekinge Institute of Technology SE - 371 79 Karlskrona Sweden, Degree Program in Information Technology,Internet Technology, 2013.

[19] Venkata Sravan Kumar, Maddineni Shivashanker Ragi, Security Techniques for Protecting Data in Cloud Computing, Master Thesis Electrical Engineering, School of Computing Blekinge Institute of Technology SE - 371 79 Karlskrona Sweden, November 2011.

[20] Uma Somani, Kanika Lakhani, Manish Mundra, Implementing the Digital Signature with RSA Encryption algorithm to Enhance the Data Security of cloud in cloud computing,1st International Conference on Parallel Distributed and Grid Computing,978-1-4244-7674-9/10, IEEE, 2010.

[21] Aman Sagar, Bineet Kumar Joshi and Nishant Mathur, A Study of Distributed Denial of Service Attack in Cloud Computing (DDoS), Edition on Cloud and Distributed Computing: Advances and Applications, Volume 2 - August 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62840-833-1.

[22] Shakti Dhar Tiwari, Mahesh Kumar and Preeti Mishra, Cloud Computing: Implementation of Software as a Service (SaaS) Multitenancy, Edition on Cloud and Distributed Computing: Advances and Applications, Volume 2 - August 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62840-833-1.

[23] Mahesh Kumar and Shakti Dhar Tiwari, Cloud Computing: Various Aspects of Cloud Security, Edition on Cloud and Distributed Computing: Advances and Applications, Volume 2 - August 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62840-833-1.

[24] Aman Sagar, Sanjeev Kumar, Palladium in Cryptography: The Advancement in Data Security, HCTL Open International Journal of Technology Innovations and Research, Volume 7, January 2014, ISSN: 2321-1814, ISBN: 978-1-62951-250-1.