# An Architecture for Data Security in Cloud Computing

**M. Sugumaran** [1]
*Dept. of Computer Science & Engineering,*
*Pondicherry Engineering College,*
*Puducherry, India*
*sugu@pec.edu*

**BalaMurugan. B** [2]
*Dept. of Computer Science & Applications,*
*Rajiv Gandhi Arts & Science College*
*Puducherry, India*
*balaanandmca@gmail.com*

**D. Kamalraj** [3]
*Dept. of Computer Science & Applications,*
*Rajiv Gandhi Arts & Science College*
*Puducherry, India*
*d.kamalrajmca@gmail.com*

***Abstract:*** **Cloud computing is a more flexible, cost effective and proven delivery platform for providing business or consumer services over the Internet. Cloud computing supports distributed service oriented architecture, multi-user and multi-domain administrative infrastructure. So, it is more prone to security threats and vulnerabilities. At present, a major concern in cloud adoption is towards its security and privacy. Security and privacy issues are of great concern to cloud service providers who are actually hosting the services. In most cases, the provider must guarantee that their infrastructure is secure and clients' data and applications are safe, by implementing security policies and mechanisms. The security issues are organized into several general categories: trust, identity management, software isolation, data protection, availability reliability, ownership, data backup, data portability and conversion, multi platform support and intellectual property. In this paper, it is discuss about some of the techniques that were implemented to protect data and propose architecture to protect data in cloud. This architecture was developed to store data in cloud in encrypted data format using cryptography technique which is based on block cipher.**

***Keywords: Cloud computing; data security; virtualization; data privacy; symmetric cryptography.***

## I. INTRODUCTION

The information technology environment has evolved from client-server, internet, virtualization, cloud computing to mainframes computers. Cloud computing provides a shared pool of configurable resources (processing, network, software, information and storage) on demand, as a scalable and elastic service, through a networked infrastructure, on a measured (pay-per-use) basis, which needs minimal management effort. This is based on service level agreements between the service provider and consumers, and often utilizes virtualization resources [14]. Cloud Computing services and products are based on an infrastructure of four core layers, namely, hardware (physical parts), software (operating systems), virtualization resources (sharing of computing resources) and applications (Salesforce.com and Google Apps). Architecture has been framed for a secured data storage based on the issues and techniques. The proposed architecture is based on cryptography algorithm, which is efficient and secured. Different experiments are done on existing algorithms and on comparing those algorithm, architecture has been designed for data security using block based symmetric cryptography algorithm. The proposed architecture uses block based symmetric cryptography having better speed of storing the data which when compared with the existing encryption algorithms. The proposed architecture encrypts the secured data by inserting the symmetric layer. This architecture is useful for the application which requires the same procedure of encryption and decryption for data storage. The service developer creates, publishes and monitors the cloud based applications and services for use by both the cloud consumer and cloud provider. The cloud has three widely used services models such as SaaS (Software as Services), PaaS (Platform as Services), IaaS (Infrastructure as Services), etc [8, 12, 13, 26, 27, 30, 32]. There are four types of cloud deployment models which are widely used as public cloud, private cloud, hybrid cloud and community cloud [32]. Public cloud represents an open access. Private cloud is operated within an organization, so that a consistent level of control over security, privacy, and governance can be maintained. Hybrid cloud is a combination of public and private cloud. It provides benefits of multiple deployment models [20, 22]. Community cloud deployment model shares resources with many organizations in a community that shares common concerns (like security, governance, compliance, etc) [20, 22, 33]. This paper discusses cloud computing in five different sections. The first section discuss the services of cloud computing and the different deployment models used to implement cloud computing. The second and third section discusses data storage issues and key technologies to implement cloud. The fourth section is about different solutions that are followed to implement data security in cloud. The fifth section explains the proposed architecture to store data securely in cloud. In the sixth section is concludes the better security.

## II. DATA SECURITY ISSUES IN THE CLOUD

Cloud computing implements three services such as SaaS, PaaS and IaaS to the end-user. In these service models different levels of security are provided in cloud computing environment. Efficient security technology in cloud computing is required to have proper secured cloud computing and to speedup cloud implementation. The security element in SaaS service model such data security, data integrity, identity management, data location, data availability, etc., are to be considered for better data security in cloud computing.

***A. Data Security and Data Protection:*** Once the client hosts 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 [15, 26, 27].

***B. Data Integrity:*** By providing security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to explain what happened to a certain dataset and at what point. It may be necessary to have exact records as to what data was placed in a public cloud. When such data integrity requirements exist, the origin and custody of data or information must be maintained in order to

978-1-4799-2877-4/14 $31.00 © 2014 IEEE
DOI 10.1109/WCCCT.2014.53



CPS Conference Publishing Services

prevent tampering or to prevent the exposure of data beyond the agreed territories [6, 10, 23].

***C. 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 location where the data are stored safely. This 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 [8]. It is often moved from one place to another place in-order to secure the data in cloud. Cloud providers have contracts with each other which are called as SLA (Service Level Agreement) and they use each others' resources [6, 8].

***D. 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. So it is important for the provider to proper data availability to the authorized user [12, 26].

***E. Identity Management:*** Each user uses his identity for accessing a cloud service. The provider should provide an identity management system for providing authentication and authorization. This is an important issue for both provider as well as user in a cloud computing environment. While providing authentication and authorization, an independent IdM stack, credential synchronization, federated IdM has implemented [24, 3].

## III. KEY DATA SECURITY TECHNOLOGIES

In cloud computing, data is stored in the third party storage. Those organization which adopt cloud computing in the world, have carried out gradually the research of cloud computing security technology, to improve the security standards of cloud computing, and ensure that organization data and personal data security. Existing security technology more reflected in the following aspects in the research field and current implementation in the industries.

***Data privacy protection:*** Data privacy protection can make an anonymous data search engine, the two interactive sides can search the data from the other side and obtain the data they need. Data privacy protection is concerned with every phase of data life cycle in cloud computing. Roy [25] put centralized information flow control (CIFC) and differential privacy protection technology into the data generation and calculation stages. Privacy protection systems which was named *airavat*, that can prevent disclosure of private data during map reduce, and can remove the key from the calculation and results automatically [3, 17, 24].

***Proof of existence and usability of data:*** Users cannot verify the correctness of data after download, as large-scale data tend to produce huge communication cost. Therefore, users have a high confidence level to determine whether the integrity of remote data. Typical work includes the following: Provable Data Irretrievability (PDR) method that user-oriented independent verification, Provable data possess (PDP) method that publicly verifiable. PDI method that was proposed by NEC laboratory improves the processing speed and expands the scale of verification object of PDR method. PDI method also supports PDP. These methods greatly improve the data security of cloud computing [4, 5, 8].

***Trusted Access Control:*** As service provider of cloud computing the implementation of user-defined access control policy must be trusted. The access control policy based on levels of key generation and distribution, attribute-based encryption algorithm, proxy re-encryption-based method, and methods that access control tree is embedded in the user key or cipher text, etc. Privileges revoked are an important issue of cryptographic-based access control policy. A basic solution is that a key is generated for set time duration. The key gets expiry after time duration and then the user updates a private key from the authority in a time intervals [8, 16]. To obtain privacy preserving in trust negotiations in cloud computing, it has propose by two techniques based on the notions of substitution and generalization. This formulates the trust negotiation requirements in terms of disclosure policies is often restrictive [2]. The trusted cloud computing platform which was named as TCCP in implementing cloud computing. Based on TCCP, IaaS service providers can offer their subscribers a closed execution environment, to ensure the confidentiality of the guest virtual machine running. In addition, it allows users to test whether the service provided by IaaS is secured before starting the virtual machine [24]. A reliable software token is developed. This token was bound with a security authentication module in order for the outsourcing sensitive (encrypted) data to perform various function operations under the condition not to disclose any information [23].

***Retrieve and process of cipher text:*** To enhance data security, you can turn the data into cipher text. But, many features lose when data was turned into cipher text. These lead most data analysis methods to failure [26, 28]. There are two typical methods to retrieve the cipher text. First, there is a safety index-based approach which checks the existence of key words by establishing a secure cipher text key words indexing. Second, there is a cipher text scanning-based approach which confirms the existence of key words and count up the number of them by matching each word in the cipher text [17, 19].

## IV. SOLUTIONS FOR DATA SECURITY IN CLOUD

Cloud computing data security refers to the set of procedures, processes and standards designed to provide information security of data in a cloud computing environment. Cloud computing data security addresses both physical and logical security issues across all the different service models and delivery models. While data of the customer need to be secured in cloud, both the data backup and data recovery methods should be efficient. The data recovery and backup process has various successful techniques. The techniques are lagging behind some critical issues like implementation of complexity, low cost, security and time related issues.

- The cloud provider should provide a proper strong encryption technique to protect the 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 for data safety [21]. The cloud seeker should be assured that data hosted on the cloud will be confidential. Towards data security, anonymity based technique for data privacy is implemented. Data security of cloud can be implemented in cloud computing by digital signature and encryption with elliptic curve cryptography [3, 27].
- CPABE (Cipher text policy attribute encryption is a mechanism for protecting the confidentiality of storing data and transmitting data information in external storage is required. Traditionally, encryption is viewed as a method for a user to share data to a targeted user or device [7]. Ensuring data storage security in cloud computing is an important aspect of Quality of Service (QoS). An effective and flexible distribution verification protocol is required to address data storage security in cloud computing. These protocols rely on erasure code for the availability, reliability of data and utilize token pre-computation using Sobol [29].
- The distributed denial of services DDOS attacks such as HTTP and XML in this environment is dangerous and provides harmful effects. These attacks can be resolved and detected by securing cloud from DDOS attacks using intrusion detection system in virtual machine [4]. HSDRT was also an efficient technique for the movable clients in cloud environment. This technique has some disadvantages. The HSDRT is an innovative file back-up concept, which makes use of an effective ultra-widely distributed data transfer mechanism and a high-speed encryption technology [9]. In Linux Box model [11] is having very simple concept of data back-up and recovery with very low cost. However, in this model protection level is very low. It also makes the process of migration from one cloud service provider to other very easy. This solution eliminates consumer's dependency on the ISP (Internet Service Provider) and its associated backup cost.
- A smart remote data backup algorithm called as Seed Block Algorithm (SBA) [18]. This algorithm is efficient in storing and retrieving data in cloud, which gets destroyed due to any reason. The time related issues are also being solved by proposed SBA such that it will take minimum time for the recovery process. SBA also focuses on the security concept for the back-up files stored at remote server, without using any of the existing encryption techniques.
- In cloud computing, VGuard framework with efficient protocol that allows a cloud policy owner and a cloud request owner to collaboratively determine, whether the request satisfies the policy without the policy owner knowing the request and the request owner knowing the policy [1].

Therefore with these techniques and solution data in the cloud computing stored securely and retrieved, from the external storage. Although each one of the backup solution and retrieved data in cloud computing is unable to achieve all the issues. Due to the high applicability of backup and retrieved process in the cloud providers and clients, need to be solved. A proposed architecture based on symmetric cryptography will be efficient technique to store and retrieve data in cloud.

## V. PROPOSED ARCHITECTURE

On comparing these issues and techniques, a new architecture has been proposed to implement the data security in cloud computing using symmetric cryptography technique. The proposed architecture is based on block based symmetric cryptography algorithm, which is very efficient and secured. Different experiment are done on existing algorithm and on comparing of those algorithm, block based symmetric cryptography algorithm is better [31]. This proposed architecture using block based symmetric cryptography has the better speed of storing data, when compared with the existing encryption algorithm. The proposed algorithm improves encryption of data secured by inserting the symmetric layer. Symmetric encryption is the oldest and best-known technique.

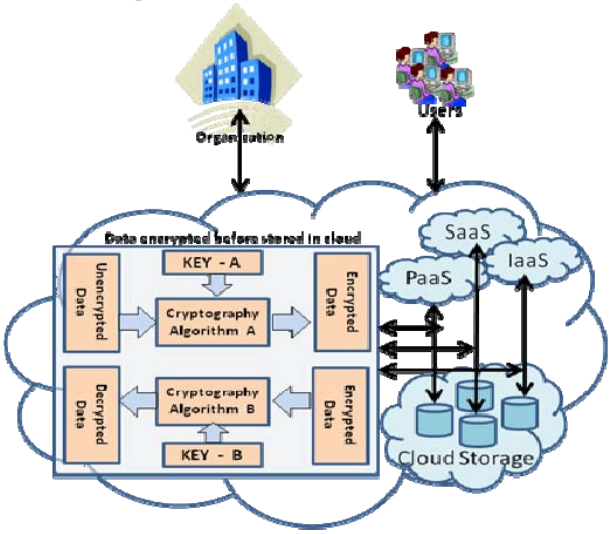


**Figure 1: Architecture for Data security in Cloud**

The secret key to generate the cipher text, which can be a number, or a word, or just a string of random block letters, is applied to the text of a message to change the content in a particular way. This cipher text may be as simple as shifting each letter by a number of places in the alphabet. As both sender and recipient know the secret key, they can encrypt and decrypt all messages that used by this key. A random number is used for generating the initial key. This key will be used for encrypting the given source file using proposed encryption algorithm with the help of encryption key number.

The symmetric encryption approach is divided into two types, one is block cipher symmetric cryptography technique and another is stream cipher symmetric cryptography. In this proposed architecture block symmetric cryptography was used, so its efficiency and security. In the proposed technique a common key was used in between sender and receiver, which is known as private key. The private key concept is the symmetric key concepts where plain text is converting into encrypted text known as cipher text using private key where

cipher text decrypted by same private key into plain text. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain private information [31].

## VI. CONCLUSION

Cloud data security encompasses a broad range of security constraints from an end-user and cloud provider's perspective, where the end-user will primarily will be concerned with the provider's data security policy, how and where their data is stored and who has access to the data. For a cloud provider, on the other hand, cloud computing data security issues can range from the physical security of the infrastructure and the access control mechanism of cloud assets, to the execution and maintenance of security policy. Cloud security is important because it is probably the biggest reason why organizations fear the cloud. To overcome these fear data security is implemented in different ways to protect the data. In cloud computing, these issues towards data security and those techniques, the proposed architecture using symmetric cryptography overcomes these issues and implement the cloud as an efficient technology for storing the customer's data.

## REFERENCES


[1] Alex X. Liu and Fei Chen, "Privacy Preserving Collaborative Enforcement of Firewall Policies in Virtual Private Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No 5, pp.887-895, 2011.

[2] Anna C and et al, "Achieving Privacy in Trust Negotiations with an Ontology-Based Approach", IEEE Transactions on Dependable and Secure Computing, Vol. 3, No. 1, pp.13-30, 2006.

[3] Arockiam, Parthasarathy and Monikandan S, "Privacy in Cloud Computing: A Survey", Proceeding of International Conference of Adv Comp Sci. & Information Technology (ACSIT 2012), pp.231-230, 2012.

[4] Asha.D and R.Chitra, "Securing cloud from ddos attacks using intrusion detection system", IJREAT International Journal of Research in Engineering & Advanced Technology, Vol 1, No.1, pp.1-6, 2013.

[5] Ateniese and et al, "Provable Data Possession at Untrusted Stores", In Proceeding of the 14th ACM Conference on Computer and Communications Security (CCS'07), ACM Press, pp.598-609, 2007.

[6] Balachandra, Ramakrishna and Rakshit, "Cloud Security Issues", IEEE International Conference on Services Computing, pp.517-520, 2009.

[7] Brent Waters, "Cipher text-Policy Attribute-Based Encryption: An Expressive, E-client, and Provably Secure Realization", 14th International Conference on Practice and Theory in Public Key Cryptography, 2011.

[8] Chirag and et al, "A Survey on Security issues and Solutions at different layers of Cloud computing", Springer Science Business Media, 2012.

[9] Chi-won and et al, "Parity Cloud Service: A Privacy-Protected Personal Data Recovery Service", Trust, security and Privacy in Computing and Communications (TrustCom) IEEE 10th International Conference, 2011.

[10] Christopher Jarabek, "A Review of Cloud Computing Security: Virtualization, Side-Channel Attacks, and Management ", from University of Calgary: http://people.ucalgary.ca/~cjjarabe/papers /jarabek_cloud_security.pdf, 2011

[11] Giuseppe and et al, "A Semantic-based System for Service Discovery in Distributed Infrastructures", 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, pp.263-272, 2010.

[12] Hoefer and G. Karagiannis, "Taxonomy of cloud computing services", Proceedings of the 4th IEEE Workshop on Enabling the Future Service-Oriented Internet (EFSOI'10), pp.1345-1350, 2010.

[13] Höfer and G. Karagiannis, "Cloud computing Services: Taxonomy and Comparison", J-Internet Server Applications, pp.81-94, 2011.

[14] HsinYi Tsai, "Threat as a Service: Virtualization's impact on Cloud Security", IT Professionals, Vol.14, No.1, pp.32-37, 2012.

[15] Kaufman. L, "Data security in the world of cloud computing", Security & Privacy, IEEE proceedings, Vol.7, No.4, pp 61-64, 2009.

[16] Leu FY and et al, "Integrating grid with intrusion detection", In Proceedings of the 19th international conference on advanced information networking and applications AINA'05, Vol. 1, pp 304-309, 2005.

[17] Mohit Marwaha and Rajeev Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", IJCSI International Journal of Computer Science, Vol.10, No.1, pp.366-370, 2013.

[18] Mowbray M and Pearson S, "A client-based Privacy Manager for Cloud Computing", In Proceedings of the fourth international ICST conference on communication system software and middleware, pp 1-8, 2009..

[19] Nagaraju Kilari and Dr. R.Sridaran, "A Survey on Security Threats for Cloud Computing", International Journal of Engineering Research & Technology, Vol.1, No.7, pp.1-10, 2012..

[20] Nashaat and Hossam, "A Proposed Model for Enhancing Data Storage Security in Cloud Computing System", Journal of Emerging Trends in Comp and Information Sci., Vol.3, pp.970-974, 2012.

[21] Parsi Kalpana and Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, Vol.1, No. 4, pp.143-146, 2012.

[22] Prashant Srivastava and et al, "An architecture based on Proactive Model for Security in Cloud computing", IEEE-International Conference on Recent Trends in Information Technology, pp.661-666, 2011.

[23] Priyanka Arora, Arun Singh and Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment" World of Computer Science and Information Technology Journal (WCSIT), Vol.2, pp.179-183, 2012.

[24] Rizwana and Sasikumar, "Security Issues in Cloud Computing A survey", International Journal of Comp. Application, Vol.4, No.19, pp.4-10, 2012.

[25] Roy, Ramadan, Setty, Kilzer, Shmatikov, and Witchel, "Airavat: Security and Privacy for MapReduce", Proceeding of the 7th USENIX Conference on networked System Designed and implementation (NSDI), pp.1-16, 2012

[26] Sharma, Sonika Soni and Swati Sengar, "Security in Cloud Computing", National Conference on Security Issues in Network Technologies types and security issue and approaches to secure data in cloud, pp.1-6, 2012.

[27] Subashini and Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol. 34, No 1, pp. 1-9, 2010.

[28] Suresh and Prasad, "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Comp Sci. and Software Engg., Vol.2, No.10, pp.110-114, 2012.

[29] Syam Kumar, Subramanian and Thanizh Selvam, "Ensuring Data Storage Security in Cloud Computing using Sobol Sequence", 1st International Conference on Parallel, Distributed and Grid Computing, pp.217-222, 2010.

[30] Vaquero and et al, "A break in the clouds: towards a cloud definition", ACM SIGCOMM Computer Communication, Vol. 39(1), 2009.

[31] 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, No. 1, January 2012.

[32] Wang Jun-jie and MuSen, "Security Issues and Countermeasures in Cloud Computing ", IEEE International Conference on Grey Systems and Intelligent Services (GSIS), pp.483-846, 2011.

[33] Wang.C, Ren.K, Lou.W and Li.J, "Toward publicly auditable secure cloud data storage services", IEEE proceeding Network, Vol.24(4), pp. 19-24, 2010.