Authentication based Hybrid Security Method for Securing Data in Cloud Environment

Sanjivani Patwa
Dept. Computer Science and Engineering
SIRTS,
Bhopal, India

Jayram Dwivedi
Dept. Computer Science and Engineering
SIRTS,
Bhopal, India

ABSTRACT

With the modern use of services of the cloud computing, the users need higher security. Therefore safety of the cloud computing is a first consideration of the users to select. In the establishment of the cloud computing, application proportion of the virtualization increases gradually, scope and the depth of safety also expanded gradually. The associated concepts of the cloud computing and its establishment conditions are discussed in this paper. In this paper the foundation of the international-certification-institute is suggested for service providing companies to raise the trust and improve the likeliness of utilizing this advance and valuable technique among the people. If the security is not fixed and powerful, then the flexibility and the benefits that a cloud computing has to provide will have the few prospect. This will facilitates the researchers and the security professionals to understand about the users concerns and the vendors concerns and the critical analysis regarding the various research types suggested.

Keywords

Component, formatting, style, styling, insert

1. INTRODUCTION

From the user's point of view, a simplest definition of the cloud-computing is to access the new functionality of rent-based-programs [1]. In the other words, the cloud-computing is a next generation of the internet-based extended version of the computing systems such that in it, resources of the computing are allowed such "as a service" [2]. The cloud-computing is a significant framework with the excellent potential in reducing the costs by enhancing and developing the functionality and the economic results that in turn may raise the pace, co-operation and the acceptance of the scalability to a conceivable degree [3].

In the cloud dependent computing framework, the resources are generally at the other's location or the network and get remotely accessed through the users of the cloud [4][5]. Processing is made remotely by applying the concept of data and the other components from a person desired to be sending to the cloud architecture or the server for its processing and the result is returned on the completion of the needed processing. In few situations, it may be needed or at least it is possible for the person to record the data on the remote cloud-servers. This technique has provided the large IT companies and the organizations with the various opportunities in the developed countries still these opportunities may suffer disputes such as security that is a main interest in the cloud computing domain [6]. If the provisions of security are not correctly and properly handled all the cloud computing domains such as the managing personal information in the public-network may comes into trouble [7, 8]. Therefore it may be claimed that the security is a key question in accepting cloud-computing. If providers may reduce this major bottle-neck, so cloud-computing will be act as pioneer in it and their acceptance through the organization and the people will be released [8].

The Cloud-Computing framework has the three types of service-delivery-models and the three major deployment models are as follows:

a. Private-cloud: When a cloud platform is committed for a particular organization.

b. Public-cloud: They are available to the public users to register and utilize the existing framework.

c. Hybrid-cloud: A private cloud which may extend to utilize the resources in the public-clouds. Public-cloud is a very susceptible deployment model as for the public users to host its services who can be the malignant users.

There are major three kinds of service within cloud environment: SaaS, PaaS, and laaS. In the cloud, same as to every suggested technique, few issues are there that included it and RAS factor is one of them.

Here are some best examples of the real time cloud-service-providers:

a. Elastic-Computing-Cloud (EC2)

This is one of the cloud-framework of the Amazon which facilitates the computational-services which enables the peoples to utilize the CPU cycles without purchasing the more computers.

b. Simple-Storage-Service (S3)

Amazon has also facilitates this service. A company called Nirvanix that is enabling the organizations to record data also the documents without adding the single on-site-server.

2. SOME POINTS RELATED WITH SECURITY

As along with the any type of storage system, some security properties are there which are required in the cloud-storage system like: integrity, confidentiality, write-serializability and the read freshness. These types of properties confirm that the data of the user is always protected and cannot be changed by the illegal users and data at the latest versions when get extracted through the user. Recording vital data with the cloud-storage-providers falls with the serious security threats. The cloud may leak the private data, change the data, or it returns the inconsistent data to the various users. This can be happen because of the crashes, bugs, operator-errors, or the mis-configurations. Additionally, the malignant security issues may be very much difficult to find or very damaging as compare the accidental ones, the external adversaries can enter into the cloud-storage-provider, or the employees of service-provider can commit an insider-attack. These aspects have protected the security conscious organization and the users from using cloud in spite of its advantages.

2.1 Problem Statement

The security and the reliability are the major challenges of the cloud-computing. The clients are not likely to allocate their data which on the cloud the data will not be get accessed through the other clients. To obtain the security on the cloud various techniques and the algorithm are available.

2.2 Cloud Security Challenges

There are following major security challenges are as follows [9]:

2.2.1 Access-Control

To examine and to promote only the authorized users, the cloud should have the right to access-control policies. These services should be well planned, adjustable and their assigning is overseeing without any difficulty. The technique governor the provision should be integrated based on the Service-Level-Agreement (SLA).

2.2.2 Authentication

Around the internet data is recorded by the cloud user is made available to all the illegal users. Therefore a certified user and the assistance cloud should have the interchangeability administration entity.

2.2.3 Service Management

In this various cloud providers like Google, Amazon, consists together to create a new made services to fulfill their customer's requirement. At this level there must be procuring divider to achieve the simplest localized-services.

2.2.4 Policy-Integration

There are various cloud-providers like Google, Amazon that are accessed by the users. Less number of conflicts in between their policies occurs because they used their own approaches and policies.

2.2.5 Trust Management

The trust-management technique should be established as the cloud environment is a service-provider and it must consist of the trust-negotiation-factor in between both the parties like the user and the provider.

2.3 Cloud Computing Security Issues

2.3.1 Layered Framework for Cloud Security

A layered framework is there which assured the security in the cloud-computing-environment. It includes of the four-layers [10]. First-layer is the secure-virtual-machine layer. Second-layer is the cloud-storage layer. This layer has the storage framework that integrates the resources from the various cloud-service-providers to create a massive-virtual storage system. And the fourth layer is the virtual-network monitor layer this layer combines both the software and hardware solutions in the virtual machines to handle the issues.

2.3.2 Components Affecting Cloud Security

Various issues of security are there for the cloud-computing as it surrounded various techniques consists of resource allocation, virtualization, transaction-management, databases, cloud networks, load balancing, operating systems, memory management and concurrency control.

2.3.3 Security Issues Faced By Cloud Computing

Cloud enables the users to obtain the power of the computing that beats their personal physical area. It directs to various issues of security. The cloud-service-provider for cloud assures that customer never suffers any issue like loss of the data or the data stolen. Cloud-computing framework uses the new services and technologies, most that have not been completely calculated according to the security. A possibility is also there in which a malignant user may enter the cloud by acting like an authorized user, by influencing the whole cloud. This directs to the affects of various users that are sharing infected cloud.

2.4 Solution for Cloud Security Issues

Few cloud security solutions are there, which the providers must keep in mind that when they are delivers their services to the cloud service users in the public-cloud-solution. Trust in between Service-provider and customer is the major issues in cloud computing. The Service-Level-Agreement (SLA) is only the legal document in between user and the service provider that includes all agreements in between user and service provider it may contains that what service provider is doing and what it is willing to do. The legal issues are also the major issues, the laws differ from country to country and the consumers have no control on where their data is located physically. Regulatory scopes such as the, data security laws and privacy laws which the cloud systems require to be follow. Preserving Integrity and the confidentiality is the big issues. Data encryption protects the improper leakage of the information.

3. LITERATURE REVIEW

A system which can gather information on cloud is suggested by this information, the kind of the security can be recognized and this outcome will make the users aware their information is protecting not risks. The implementation of the system is dependent on considerably small clouds therefore extending of this architecture is needed [10]. Dependent on properties of the security in between the analysis and the applications of the data management then a data-centric architecture of the cloud security is suggested. The merit of this architecture is represented by using the Declarative-Secure-Distributed Systems platform. Various directions are further establishment of this paper [11]. Dependent to features of major privacy and security issues in cloud-computing, four efficient approaches are suggested. These approaches can work with the one or the two aspects like privacy and security issues [12].

In paper [13] it shows excellent resource management architecture for cloud-computing environment. Dependent on the virtualization technique, the workload to be processed on the virtual-machine may be moved that is out-sourced from the private-cloud that is the in-house computer system to service provider in the public-cloud. The architecture introduces a virtual-machine-manager (VMM) in the private-cloud operating to reduce the cost because of the out-sourcing and the performance decline. An assumed optimization model is established to achieve an excellent workload out-sourcing policy along with the target to reduce the cost. The numerical studies disclose the efficient behavior of the optimal resource-management architecture to obtain the target of the private-cloud. Their architecture will be useful to enhance the performance of the resource usage, but also to obtain best advantages from the economic aspect of cloud-computing management.

In this paper [14] offers a closer observation at cloud-computing-services. It first developed a baseline through specifying the high level need for the cloud-computing services. Next it enhances on present framework for cloud-computing services through adding the new modules to a recent framework. The new modules are collected from the analysis of telecommunications security and cloud in the distributed-systems. The modern modules consist of the management and the control network, the set of the trust domains, and the set of the proxies. Cloud computing technique was the new idea of offering the bandwidth, dramatically virtualized and scalable resources, hardware and software on demand to the consumers. The consumers could normally requests the cloud services through a web service or web browser. By using the cloud computing, the consumers can protect the cost of the hardware deployment, the software licenses and maintenance of the system.

On the contrary, it has also some security-issues. In paper [15] introduced the four major cloud security issues, that are Browser Security, XML Signature Element Wrapping, Cloud Malware Injection Attack and the Flooding Attacks, and they also gives a possible counter measures.

In paper [16] it is discussed the performance of the six symmetric key-RSA data encryption algorithms in the cloud-computing-environment. They have suggested the two different cloud-servers; one for the data server and the other for the key cloud-server and data encryption and the decryption operate at a client-side. The major demerit of this approach is maintaining the two different servers for the security of data in the cloud that made a large storage and the more computation overheads.

In the paper [17] suggested the cloud computing is a versatile technique which may support the broad-range of the applications. This paper, analyzes the various concepts included in the cloud computing. Cloud-computing is not only the application dependent but also it is service oriented, it provided on demand virtualization of resources as the billable and measurable utilities. The minimum cost of the cloud computing and their dynamic scaling contribute it an innovation-driver for the small companies, especially in developing the world. The summary of analysis done by them on basic problems of cloud-computing such as the performance, security, availability, regulatory requirements, cost, quality of service, Bandwidth and the data limits.

Security is a much prioritized concept for any form of the computing, building it an apparent expectation that the security problems are complicated for the cloud-environment also. As cloud-computing technique can be relate with having the users' private data recorded both at the clients end and also in the cloud servers, authentication and identity management are very complicated in the cloud-computing [18][19][20] Verification of the able user's credentials and securing these credentials are the part of the major issues of security in cloud - violation within these areas can directs to the undetected security issues [21] at least to few extent for limited time.

Various modes of the data transfer and the communication means may require to be considered. Large volume of the data transfer is the common expectation in the cloud environment, the communication technique is used with security aspects of accepted communication technique have also becomes the security matter for cloud-computing method. The behavior of broadcast of the few techniques of communication is the core aspect in this term [22]. The cloud environment is related with both the virtual and physical resources and they have separate level of the security problems – that are having no complicated authentication approach to fully refer the security risks is the present issue for the cloud-computing. It mainly has found in the conditions in which grid-computing has been considered as an embedded portion of the cloud-computing [23].

4. PROPOSED WORK

There is variety of works for providing security to cloud storage data. Here the proposed flow chart is given in fig 1.

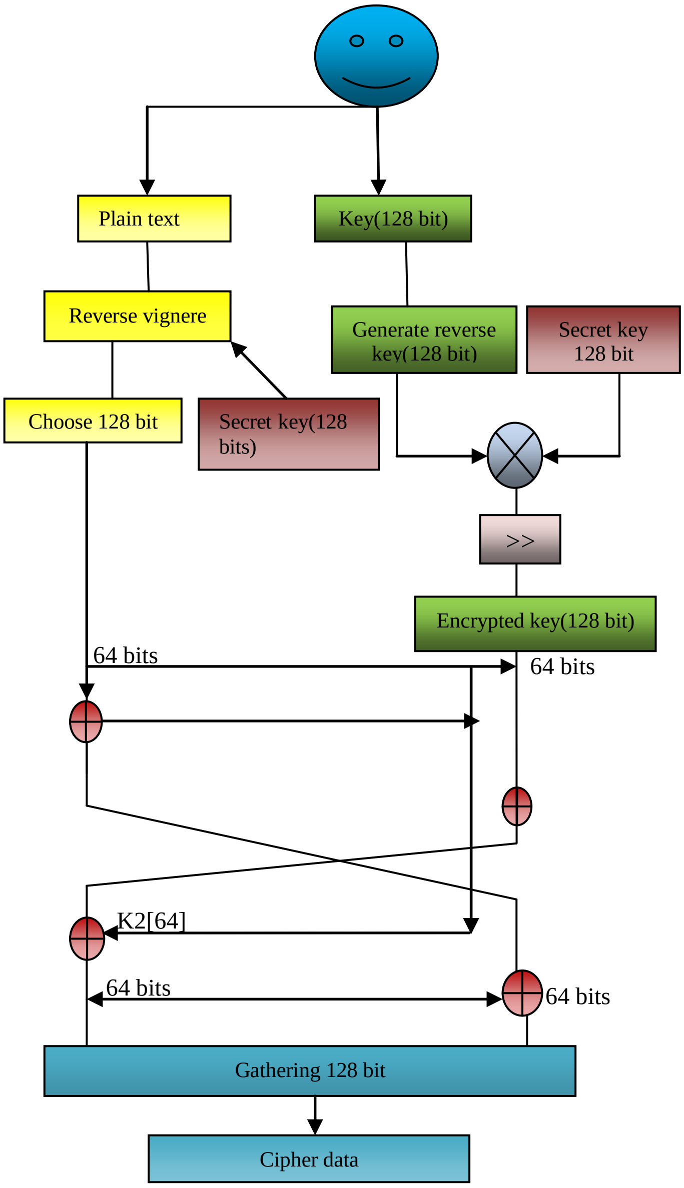


Fig 1: Proposed Flow Chart

It is very easy to see that the proposed work contents following features:

1. Reverse Vignere
2. Encryption Algorithm with 128 bit key
3. Attribute Based Encryption for Authentication

Reverse Vignere gives the benefit of stream ciphering while another block of 128 bits encryption gives benefit of block ciphering. It is already know fact that higher length block encryption algorithm is hard to break as compare to the short length algorithm. At the another end this encryption algorithm will become more secure by providing authentication beside of simply encryption. This authentication is done by Attribute based Cryptography.

Step 1: First of all, users send the plain text and generate the Key of 128 Bits.

Step 2: Then we generate Reverse Key and Secret Key from generated Key by applying Generate Reverse Key Algorithm (128 Bits).

Step 3: We use XOR Operation for encrypt the data and also apply Right Bit Shift Operator.

Step 4: It generates Encrypted Key of 128 Bits.

Step 5: We will apply Reverse Vignere Algorithm, for convert Plain Text to Cipher Text with Secret Key of 128 Bits.

Step 6: We will choose First 128 Bits and divide into 64 - 64 Bits.

Step 7: The Encrypt Key also divides into 64 -64 bits, exchange both the Key apply XOR Operation for K1 [64] Bits and same with K2 [64] Bits.

Step 8: Then after both Key of 64-64 Bits will be gathered in 128 Bits.
Step 9: We will receive Cipher Data of 128 Bits.

5. RESULT ANALYSIS

The proposed work has been improved the efficiency and effect of the security. These things are proved based on following parameters:

1. Decryption Time
2. Avalanche Effect

The system which is used to perform and evaluate this proposed work over existing work is as follows:

Table 1: System Configuration

OS	**Win7 with 32 bits**
Processor	Dual Core
RAM	4GB

String and key which are considered for our experiments are as follows:

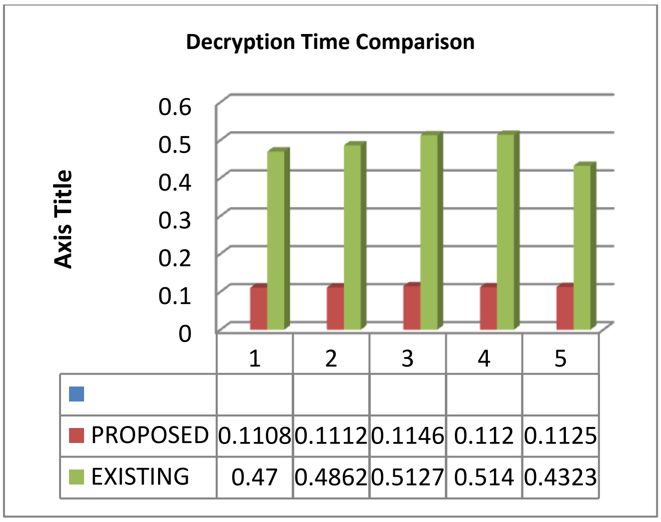
String: The quick brown fox Jumps over the lazy dog

Key: Showtimesecurity

Avalanche Key: Showtimesecuriti

Table 2: Comparison of Decryption time

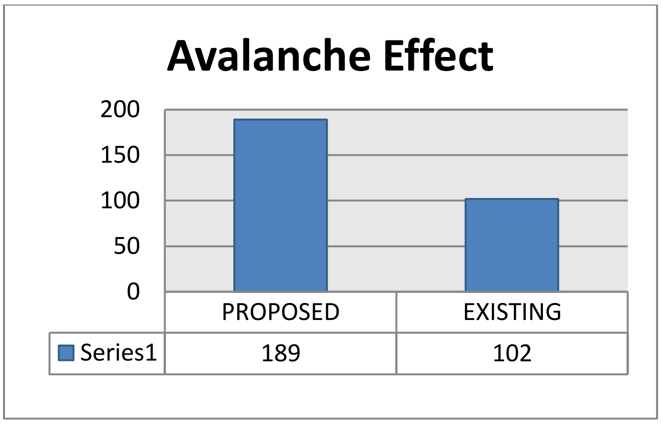
S. No.	PROPOSED	EXISTING
1	0.110759	0.469974
2	0.111186	0.486224
3	0.114607	0.512738
4	0.112041	0.514021
5	0.112469	0.432342



Graph 1: Comparison of Decryption time

Table 3: Comparison Avalanche Effect

PROPOSED	EXISTING
189	102



Graph 2: Comparison Avalanche Effect

6. CONSLUSION

In current global market of competition, the organization should introduce and obtained most from their resources to get succeed. This needs enabling its business partners, employees and the users along with platforms and the collaboration mechanism which promote the innovation. The cloud computing architectures are the next-generation platforms which may offers the tremendous value to the companies belonging to any size. The cloud-computing offers Platform, Software, Storage, Infrastructure, Data, Security, Test Environment etc. as a service. In this paper the various security problems have been discussed of the cloud-computing and also regarding the cloud-computing. Here also explain few already exists cloud-security-solutions by the few researchers. There are various other challenges regarding the security concept of the cloud-computing have been discussed. Various solutions are available for these challenges in the cloud-computing, vendors, stakes holders, organizations and enterprises may have to think seriously regarding the security matters of the cloud-computing before accepting cloud-system. Graph 1 and 2 along with Table 2 and 3 easily show that the performance of the proposed work is much better than existing work.

7. REFERENCES

[1] Yashpal Kadam, "Security Issues in Cloud Computing A Transparent View", International Journal of Computer Science & Emerging Technologies, Vol-2 No 5 October, 2011.

[2] Mohamed Al Morsy, John Grundy and Ingo Müller, "An Analysis of The Cloud Computing Security Problem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30 Nov 2010.

[3] H. Takabi, J.B.D. Joshi, G.Ahn., "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security Privacy Magazine, Vol 8, IEEE Computer Society, p.24-31, 2010.

[4] Petre, R. (2012). Data mining in Cloud Computing. Database Systems Journal, 3(3), 67-71.

[5] Ogigau-Neamtiu, F. (2012). Cloud Computing Security Issues. Journal of Defense Resource Management, 3(2), 141-148.

[6] M. Monsef, N. Gidado, "Trust and privacy concern in the Cloud", 2011 European Cup, IT Security for the Next Generation, p.1 -15, 2011.

[7] M. Firdhous, O. Ghazali, and S. Hassan, Trust and Trust Management in Cloud Computing – A Survey, Inter Networks Research Group, University Utara Malaysia, Technical Report UUM/CAS/InterNetWorks/TR2011-01, 2011.

[8] Farhad Soleimanian Gharehchopogh, Sajjad Hashemi, "Security Challenges in Cloud omputing with More Emphasis on Trust and Privacy", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, Vol. 1, ISSUE 6, pp. 49-54. 2012.

[9] Chandrahasan, R. Kalaichelvi, S. Shanmuga Priya, and L. Arockiam. "Research Challenges and Security Issues in Cloud Computing." International Journal of Computational Intelligence and Information Security 3.3 (2012): 42-48.

[10] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International
Journal of Information Security and Privacy, 4(2), 39-51, University of Texas, USA, April-June 2010.

[11] Z. Wang, "Security and Privacy Issues within the Cloud Computing,"2011 International Conference on Computational and Information Sciences, (2011), pp. 175–178.

[12] J. C. Roberts II and W. Alhamdani, "Who Can You Trust in the Cloud?: a Review of Security Issues within Cloud Computing", ACM International Security Curriculum Development Conference, (2011), pp. 15–19.

[13] Dusit Niyato," Optimization-Based Virtual Machine Manager for Private Cloud Computing", Third IEEE International Conference on Coud Computing Technology and Science, 2011.

[14] Abdur Rahim Choudhary," Baseline Requirements and Architecture for Cloud Computing Services", International Journal of Advanced Computer Research (IJACR) ,Volume-2 Number-4 Issue-7 December-2012.

[15] Danish Jamil, Hassan Zaki, Security Issues In Cloud Computing And Countermeasures, International Journal of Engineering Science
and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011

[16] ShivShakti etc(2013 January-Febuary)."Encryption using different techniques:A Review" international journal in Multidisciplinary and academic research (SSIJMAR) vol.2 No.1 - (ISSN 2278-5973).

[17] J.Srinivas, K.Venkata Subba Reddy, Dr.A.Moiz Qyser(2012 july)"Cloud Computing Basics" International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 1, Issue.

[18] Emam, A.H.M. (2013). Additional Authentication and Authorization using Registered Email-ID for Cloud Computing. International Journal of Soft Computing and Engineering, 3(2), 110-113.

[19] Han, J., Susilo, W. and Mu, Y. (2013). Identity-based data storage in cloud computing. Future Generation Computer Systems, 29, 673–681. doi:10.1016/j.future.2012.07.010

[20] Yassin, A.A., Jin, H., Ibrahim, A., Qiang, W. and Zou, D. (2012). Efficient Password-based Two Factors Authentication in Cloud Computing. International Journal of Security and Its Applications, 6(2), 143-148.

[21] Kumar, A. (2012). World of Cloud Computing & Security. International Journal of Cloud Computing and Services Science, 1(2), 53-58.

[22] Celesti, A., Fazio, M., Villari, M. and Puliafito, A. (2012). Virtual machine provisioning through satellite communications in federated Cloud environments. Future Generation Computer Systems, 28, 85–93. doi:10.1016/j.future.2011.05.021

[23] Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). The Cloud Grid approach: Security analysis and performance evaluation. Future Generation Computer Systems, 29, 387–401.