International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-3, March 2016
ISSN: 2395-3470
www.ijseas.com

Trusted Cloud Computing Methods using to Protected File Encryption Performance

Sivakumar K
Assistant Professor (Sr.G)
JCT College of Engineering and Technology,Coimbatore.
sivakumar_srec@yahoo.com

Abstract

In private cloud system, data is shared among the persons UN agency square measure therein cloud. For this, security or personal data concealing method hampers. though Cloud computing has achieved an excellent success in varied industries whether or not it's a software package trade, during this paper we've got projected new security design for cloud computing platform. the shoppers in faithfully distinguishing trustworthy cloud suppliers multi-faceted Trust Management (TM) system design for a cloud computing marketplace is additionally attainable to let technical agents monitor every other's behavior and respond consequently by increasing or decreasing trust. It ensures secure communication system and concealing data from others. during this system give Blowfish algorithmic rule for file secret writing and RSA primarily based secured communication. During this paper deals with varied problems related to Security and focus in the main on the info security and strategies of providing security by encryption. varied secret writing strategies of block cipher algorithms like RSA, Blowfish square measure mentioned for providing solutions to cloud security. The system exploitation totally different key for each secret writing and coding and increasing overall performance of cloud service supplier exploitation Fair-Share hardware. that the customers simply determine a decent or poor quality cloud supplier.

Keywords: *Cloud Computing, Trust management, CAIQ, Blowfish, RSA, Fair Share Scheduler, Virtual Machine Monitoring, Performance.*

1. Introduction

Cloud computing is the concept of using remote services through a network using various resources. It is basically meant to give maximum with the minimum resources i.e. the user end is having the minimum hardware requirement but is using the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way. Clouds are of particular commercial interest not only with the growing to outsource IT so as to reduce management overhead and to extend existing, limited IT infrastructures, but even more importantly, they reduce the entrance barrier for new service providers to offer their respective capabilities to a wide market with a minimum of entry costs and infrastructure requirements in fact, the special capabilities of cloud infrastructures allow providers to experiment with novel service types at the same time reducing the risk of wasting resources. Cloud is not only simple collecting the computer resource, but also provides a management mechanism and can proide services for millions of users simultaneously. Cloud computing is the broader concept of infrastructure convergence. This type of data centre environment allows enterprises to get their applications up and running faster, with easier manageability and less maintenance to meet business demands.

A. Data Verification in Cloud

Verification of personnel's competence Verification of team's procedures and policies Verification of financial stability and sustainability Verification of basic operational factors, such as: reach ability or response times. In order to complete the certification, the team should sign a code of conduct, specifying expectations the team would commit to meet, such as vulnerability disclosure policy, response times, etc. As the business market is growing rapidly with new providers entering the market, cloud providers will increasingly compete for customers by providing services with similar process.

However, there can be huge differences regarding the provided quality level of those services. Such a competitive market needs means to reliably assess the quality level of the service providers. The term “trust” is often loosely used in the literature on cloud trust, frequently as a general term for “security” and “privacy”, What exactly does “trust” mean? Trust is a complex social phenomenon. Based on the concepts of trust developed in social sciences.

Iteration	Action Behavior	AN	Total	V
1	Positive	0	1	1
2	Malicious	1	2	0.4
3	Positive	1	3	0.7
4	Malicious	2	4	0.4
5	Malicious	3	5	0.3

Table 1: Trust Value Based Information

Trust is a mental state comprising: expectancy – the trustor expects a specific behavior from the trustee (such as providing valid information or effectively performing cooperative actions); belief - the trustor believes that the expected behavior occurs, based on the evidence of the trustee’s competence, integrity, and goodwill; willingness to take risk - the trustor is willing to take risk for that belief.

To create a trust management system with using different attributes based on the Service Level Agreement. This SLA provides assurance between cloud service provider and customer. In this system provide secure authentication with frequent questions and answers. Then also minimizes response time and workload with using Fair-Share Scheduler.

II. SECURITY SLA MANAGEMENT FOR THE CLOUD

A service is a means of delivering value to customers. A service represents some function or type of task performed by a provider on behalf of a customer. Cloud computing services benefit from economies of scale achieved through versatile use of resources, specialization, and other efficiencies. However, it is an emerging form of distributed computing still in its infancy. Cloud computing can be implemented entirely within an organizational computing environment as a private cloud. However, it should be clear from the service models described that a main thrust of cloud computing is to provide a means to outsource parts of that environment to an outside party.

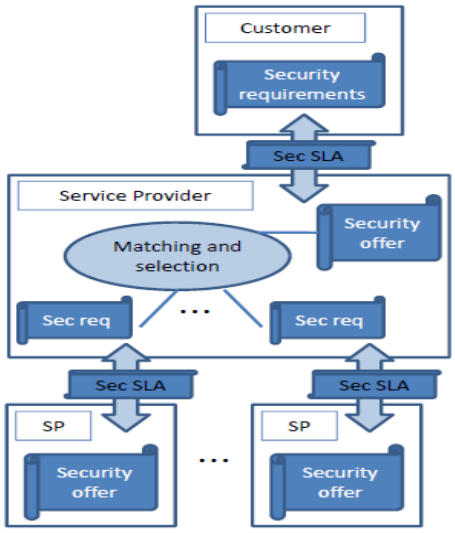

Fig 1: The Security SLA

A challenging part of the security SLA process lifecycle is to agree on what specific security mechanisms to include in the agreement. We have previously outlined a framework for security mechanisms in SLAs for Cloud services.

III. CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE

The CAIQ engine allows cloud providers to fill in the CAI questionnaire by providing an intuitive graphical interface through the RM. The questionnaire helps cloud providers to represent their competencies to the potential users with respect to different attributes. When a user login the system at time CAIQ engine will get the question and answer from the user and check authentication. If question and answer is valid means it provide access permission to user otherwise return the previous login page. This CAIQ provide secure authentication.

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. It fills in the CAI questionnaire as a part of cloud policy. Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the service provider.

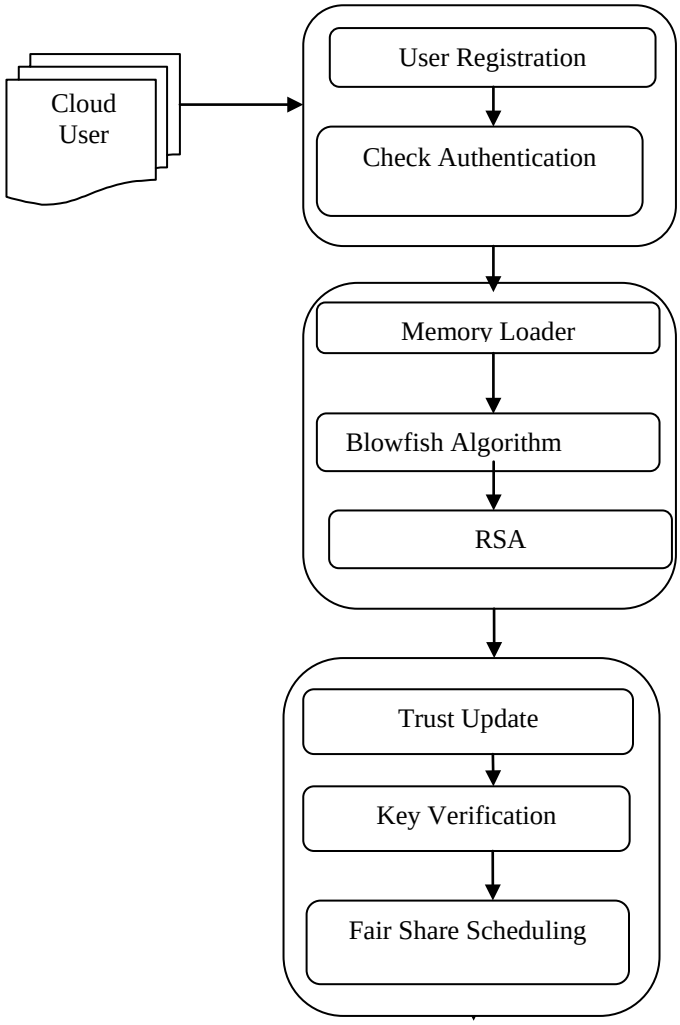

Fig 2: System Architecture

This architecture will react the multi-faceted nature of trust assessment by considering multiple at-tributes, sources and roots of trust. It aims at supporting customers to identify trustworthy services providers as well as trustworthy service providers to stand out. The user is trying to locate a number of documents which together will provide the desired information. The associate rule convert every trust relevant information into propositional logic terms with using trust semantic or computational.

At present, although cloud providers demonstrate their preventive measures by including related descriptions in the SLAs, assurances and compensations for SLA violations are not convincing enough for the consumers. Especially, SLAs with vague clauses and unclear technical specifications lead the consumers into a decision dilemma when considering them as the only basis to identify trustworthy providers.

The trust management is an abstract system that processes symbolic representations of social trust, usually to aid automated decision-making process. The trust manager allows cloud users to specify their requirements and opinions when accessing the trust score of cloud providers.

Semantic search seeks to improve search accuracy by understanding searcher intent and the contextual meaning of terms. The TSE are considered to be the expected behavior of a cloud provider in terms of a specific attribute. The TSE should be able to convert every trust relevant information into propositional logic terms.

IV.FAIR-SHARE SCHEDULING ALGORITHM

Fair-share scheduling is a scheduling strategy for computer operating systems in which the Virtual Memory usage is equally distributed among system users or groups, as opposed to equal distribution among processes. The Completely Fair Scheduler (CFS) is the name of a process scheduler which was merged into the 2.6.23 release of the Linux kernel. It handles VM resource allocation for executing processes, and aims to maximize overall VM utilization while also maximizing interactive performance.

The scheduler stores the records about the planned tasks in a red-black tree, using the spent processor time as a key. The most common was to simply assign weights to users such that one user may get twice as many time slices in a given time period as others. The entry of the picked process is then removed from the tree, the spent execution time is updated and the entry is then returned to the tree where it normally takes some other location.

- Total memory size of VM / Number of available users= per user.

If there are three VM's (1,2,3) containing three, two, and four users respectively, the available size will be distributed as follows:

- ✓ 100% / 3 groups = 33.3% per VM
- ✓ VM 1:(33.3% / 3 users)=11.1% per user
- ✓ VM 2:(33.3% /2 users) =16.7% per user
- ✓ VM 3:(33.3% /4 users) = 8.3% per user

A. Fair-Share Parameters

Fair-share scheduling allows utilization targets (i.e., shares) to be set for users, groups, and classes. The target utilization is based on the usage during "windows" of time, and shares can be configured at the system level, at the group level, and at the user level. The dynamic priority of a job is a calculation based on the proportion of the target utilization that has been used. This allows it to pick efficiently the process that has used the least amount of time.

- FS_INTERVAL

- FS_DEPTH
- FS_DECAY

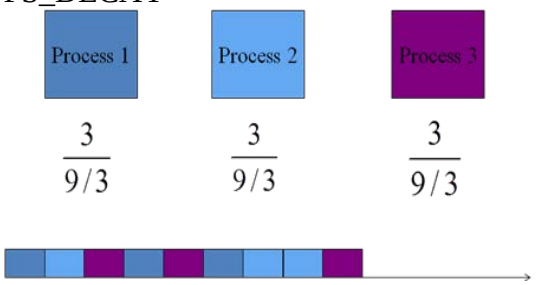

Fig 4: Fair- Share scheduler Example

It handles VM resource allocation for executing processes, and aims to maximize overall VM utilization while also maximizing interactive performance. The scheduler stores the records about the planned tasks in a red-black tree, using the spent processor time as a key.

Workload characterization is a process to construct a concise description of the workload based on the input trace data and other information that may be known about the execution environment. The trade-off in workload characterization is between complexity and predictive power. While the original trace data set contains very detailed information about the user load that is placed on the cluster system, it is difficult to construct a prediction workload from the trace data alone. Factors such as the number of nodes requested by a particular job, the overall run time, and the amount and rate of data read or written may not be uniform over a measurement period.

B. Workload Modeling

Workload modeling always starts with measured data about the workload. This is often recorded as a trace, or log, of workload-related events that happened in a certain system. The workload trace for this paper is a workload trace that has been acquired from the job scheduler monitoring system of two kinds of clusters: Acxiom Corporation Cluster and University of Arkansas Red Diamond Supercomputer.

The focus of the research is on analyzing the effects of modifying various parameters of fair-share scheduling policy on the performance of classes user jobs with different characteristics. The focus is not on determining whether the achieved effect is more or less “fair” to one user group or another, which is generally a business decision for the operation of the overall enterprise.

C. Revising Priorities

$$Pr_j(i) = Base\_Pr_j + \frac{CPU_j(i)}{2} + \frac{GCPU_k(i)}{4 * W_k}$$

$$CPU_j(i) = \frac{CPU_j(i-1)}{2} + \frac{U_j(i-1)}{2}$$

$$GCPU_j(i) = \frac{GCPU_k(i-1)}{2} + \frac{GU_k(i-1)}{2}$$

In this case, the available VM cycles are divided first among the groups, then among the users within the groups, and then among the processes for that user. updated and the entry is then returned to the tree where it normally takes some other location.

V. BLOWFISH ALGOTRITHM

Blowfish is a symmetric block cipher encryption algorithm meaning that it uses the same secret key to both encrypt and decrypt messages and divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. It takes a variable length key, from 32 bits to 448 bits, making it ideal for securing data. It is suitable for applications where the key does not change often, like a communications link or an automatic file

encryption. It is significantly faster than most encryption algorithms when implemented on 32 bit microprocessors with large data caches.

Finding the plain text of an encrypted message without knowing the key is called "cracking" an algorithm. This brute-force attack consists of trying all possible values of keys until the right one is found.

A. Encryption

Blowfish is a Feistel network consisting of 16 rounds The input is a 64.Blowfish is also one of the fastest block ciphers in public use, making it ideal for a product like SplashID that functions on a wide variety of processors found in mobile phones as well as in notebook and desktop computers

bit data element, x:
Blowfish has 16 rounds.
The input is a 64-bit data element, x.
Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16:
xL = xL XOR Pi
xR = F (xL) XOR xR
Swap xL and xR
After the sixteenth round, swap xL and xR again to undo the last swap.
Then, xR = xR XOR P17 and xL = xL XOR P18

B. Decryption

Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption.The P array consists of 18 32 bit subkeys : P1, P2,..., P18.There are four 32 bit S boxes with 256 entries each:

S1,0, S1,1,..., S1,255;
S2,0, S2,1,..,, S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..,, S4,255.

VI. RSA ALGORITHM

The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. RSA is an algorithm for public key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. The basic steps of RSA algorithm are:

- Key Generation
- Encryption and
- Decryption

The RSA algorithm is used for secured communication between the users and the servers. This paper is formatted in the following way: section II describes related work of this paper work, section III describes proposed architecture and its working steps, section IV describes the experimental environment, results in different aspects and advantages of the proposed model, and section V describes the future aspects related to this paper work.

The algorithm involves multiplying two large prime numbers and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key.

In the proposed model RSA encryption algorithm is used for making the communication safe. Usually the users requests are encrypted while sending to the cloud service provider system. RSA algorithm using the system's public key is used for the encryption. Whenever the user requests for a file the system sends it by

encrypting it via RSA encryption algorithm using the user's public key.

Same process is also applied about the user password requests, while logging in the system later. After receiving an encrypted file from the system the user's browser will decrypt it with RSA algorithm using the user's private key. Similarly when the system receives an encrypted file from the user it will immediately decrypt it using its private key. As a result the communication becomes secured between the user and the system.

VII. RELATED WORK

In the work [1] Identity-Based Cryptography (IBC) is in a very quick development [6, 7]. Identity-Based Encryption (IBE) provides a public key encryption mechanism where a public key is an arbitrary string such as an email address or a telephone number [17, 18]. The corresponding private key can only be generated by a Private Key Generator (PKG) who has knowledge of a master secret. Using this construct, anyone can encrypt messages or verify signatures without prior key distribution beyond the dissemination of public parameters and the public key "strings." This is useful where the deployment of a traditional certificate authority-based PKI is inconvenient or infeasible, as IBE-based systems do not require certificate management.

In the work [2] Reputation systems can be tricked by the spread of false reputation ratings, be it false accusations or false praise. Simple solutions such as exclusively relying on one's own direct observations have drawbacks, as they do not make use of all the information available. In propose a fully distributed reputation system that can cope with false disseminated information. Further, a key challenge formultiagent systems is how to determine trust based on reports from multiple sources, who might themselves be trusted to varying degrees. We are finding that customers with security-critical data processing needs are beginning to push back strongly against using cloud computing. . Thus, reputation ratings are slightly modified by accepted information in trusted cloud computing environment process.

In the work [3] Trust should be substantially based on evidence. Further, a key challenge formultiagent systems is how to determine trust based on reports from multiple sources, who might themselves be trusted to varying degrees. Hence an ability to combine evidence-based trust reports in a manner that discounts for imperfect trust in the reporting agents is crucial for multiagent systems In cloud computing, a vendor runs their computations upon cloud provided VM systems. These include referral systems and webs of trust in particular, in studying which we identify the need for this research.

In the work [4] Cloud computing is a new computing model, and security is ranked first among its challenges. This paper reviews existing security monitoring mechanisms compared with new challenges which are caused by this new model. We highlight possible weaknesses in existing monitoring mechanisms, and propose approaches to mitigate them From time to time first-hand reputation information is exchanged with others. To using a modified Bayesian approach we designed.

CONCLUSION AND FUTURE ENHANCEMENT

The core concept of this paper is consistent with division of management authority to reduce operational risk, thus avoiding the risk of wrongful disclosure of user data. New cloud providers are entering the market with huge investments and the established providers are investing millions into new data centers around the world. At present, it is extremely difficult for cloud customers to tell the difference between a good and poor quality cloud provider and believe that taking into account this standardized

questionnaire lowers the entrance barrier for cloud providers and provide assurance to the user with using questionnaire and Fair-Share Scheduler.

The data storage security in Cloud Computing, an area full of challenges and of paramount importance, are still in its infancy now, and many research problems are yet to be identified is to enhance the more security features by using other enhanced techniques of data security through cryptosystems and other techniques. cloud computing does provide us with tangible benefits but today we still have no definite answers on a proper security platform for cloud computing, only suggestions and being formed but we are yet to see a practical security measure for cloud computing to be a safer platform for organizations and individuals. T

REFERENCES

[1]. Sheikh Mahbub Habib, Sebastian Ries, Max Muhlhauserz(2011), “Towards a Trust Management System for Cloud Computing”, published by the IEEE 10th International Conference on Trust, IEEE Computer Society.

[2]. Tingyuan Nie,Chuanwang Song, Xulong Zhi(2010),Performance Evaluation of DES and BlowfishAlgorithms', Biomedical Engineering & computer science, InternationalConference.

[3]. Debajyoti Mukhopadhyay, Gitesh Sonawane, Parth Sarthi Gupta, Sagar Bhavsar, Vibha Mittal (2013), “ Enhanced Security for Cloud Storage using File Encryption ”.

[4]. Simar Preet Singh(2011), Comparison of Data Encryption Algorithm, IJCSC, Vol 2 No.1, June

[5]. Habib.S.M, Ries.S, and Muhlhauser.M (2010), “Cloud computing landscape and research challenges regarding trust and reputation," Symposia and Workshops on ATC/UIC, pp. 410- 415.

[6]. Haq.I.U, Alnemr.R, Paschke.A, Boley.H, and Meinel.C (2010), “Distributed trust management for validating sla choreographies," in Grids and Service-Oriented Architectures for Service Level Agreements. Springer US, pp. 45-55.

[7]. Nagarajan.A and Varadharajan.V (2011), “Dynamic trust enhanced security model for trusted platform based services," Future Gener. Computes. Syst., vol. 27, pp. 564573.

[8]. Ries.S, Habib.S.M, and Varadharajan.V (2011), Certainlogic: “A logic for modeling trust