REPUTATION MANAGEMENT MECHANISM AND SECURITY IN FEDERATED CLOUD

[1]Sridevi. S, [2]Thenmozhi.V, [3]Valarmathi.K, [4]Gracy Therasa.W

[1,2,3]UG Scholar, [4]Associate Professor Department of CSE,
AdhiyamaanCollege of Engineering,Hosur,TN,India
[1]sridevisrinivasan27@gmail.com, [2]thenmozhivenkateshan128@gmail.com,[3]valarkrishnan97@gmail.com, [4]sunphin14@gmail.com

ABSTRACT - The Reputation Management mechanism is a mechanism of managing the reputed cloud. It is used to find the standardized and reputed cloud in the cloud world. The reputation of the cloud is found through the feedback given by the user which is differentiated by the ++trust manager. Through this the user can be able to purchase the reputed cloud. Trust management is one of the most challenging issues for the adoption and growth of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability. Preserving consumers' privacy is not an easy task due to the sensitive information involved in the interactions between consumers and the trust management service. Protecting cloud services against the malicious users (e.g., such users might give misleading feedback due to this reputation of the cloud provider will be reduced) is a difficult problem, for this Greedy Algorithm is used to separate the good and malicious user. The security for the data stored by the user is given by Advanced Encryption Standard (AES) Algorithm. User can store the data in the Cloud in a secured manner. The data stored by the user will be stored in an encrypted form using Advanced Encryption Standard (AES) Algorithm. The data will encrypted while uploading the file in the cloud and the data will be decrypted while downloading the file.

Keywords: Cloud Provider, Trust Manager, Greedy Algorithm, AES Algorithm.

1. INTRODUTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

Working of Cloud Computing: The goal of cloud computing is to apply traditional supercomputing, or high- performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second,in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large,immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Characteristics: The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

On-demand self-service:A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Advantages:
Price: Pay for only the resources used.

Security: Cloud instances are isolated in the network from other instances for improved security.

Performance: Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's

Scalability: Auto-deploy cloud instances when needed.

Uptime: Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.

Control: Able to login from any location. Server snapshot and a software library lets you deploy custom instances.

Traffic: Deals with spike in traffic with quick deployment of additional instances to handle the load.

2. 2.LITERATURE SURVEY

Y. Azar, S. Kamara, I. Menache, M. Raykova, and B. Shepard, "Colocation-resistant clouds," in Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security, ser. CCSW '14. New York, NY, USA: ACM, 2014, pp. 9–20.

It consider the problem of designing multi-tenant public infrastructure clouds resistant to cross-VM attacks without relying on single-tenancy or on assumptions about the cloud's servers. In a cross-VM attack (which have been demonstrated recently in Amazon EC2) an adversary launches malicious virtual machines (VM) that perform side-channel attacks against co-located VMs in order to recover their contents.

This paper propose a formal model in which to design and analyze *secure* VM placement algorithms, which are online vector bin packing algorithms that simultaneously satisfy certain optimization constraints and notions of security. It introduce and formalize several notions of security, establishing formal connections between them. It also introduce a new notion of efficiency for online bin packing algorithms that better captures their cost in the setting of cloud computing. Finally, this propose a secure placement algorithm that achieves our strong notions of security when used with a new cryptographic mechanism it refer to as a shared deployment scheme [3].

J. Huang and D. Nicol, "Trust mechanisms for cloud computing," Journal of Cloud Computing, vol. 2, no. 1, 2013.

Trust is a critical factor in cloud computing; in present practice it depends largely on perception of reputation, and self assessment by providers of cloud services. This paper begin with a survey of existing mechanisms for establishing trust, and comment on their limitations. It then address those limitations by proposing more rigorous mechanisms based on evidence, attribute certification, and validation, and conclude by suggesting a framework for integrating various trust mechanisms together to reveal chains of trust in the cloud [2].

Mahmoud M.M and Shen .X,(2012) "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805–1818.

In wireless sensor networks, adversaries can make use of the traffic information to locate the monitored objects, e.g., to hunt endangered animals or kill soldiers. This paper, first define a hotspot phenomenon that causes an obvious inconsistency in the network traffic pattern due to the large volume of packets originating from a small area. Second, it develops a realistic adversary model, assuming that the adversary can monitor the network traffic in multiple areas, rather than the entire network or only one area. Using this model, it introduces a novel attack called Hotspot-Locating where the adversary uses traffic analysis techniques to locate hotspots. Finally, this paper propose a cloud-based scheme for efficiently protecting source nodes' location privacy against Hotspot-Locating attack by creating a cloud with an irregular shape of fake traffic, to counteract the inconsistency in the traffic pattern and camouflage the source node in the nodes forming the cloud.

To reduce the energy cost, clouds are active only during data transmission and the intersection of clouds creates a larger merged cloud, to reduce the number of fake packets and also boost privacy preservation. Simulation and analytical results demonstrate that scheme can provide stronger privacy protection than routing-based schemes and requires much less energy than global-adversary-based schemes [1].

Shen.Q, Liang.X, Shen.X, Lin.X, and Luo.X,(2014) "Exploiting geodistributed clouds for e-health monitoring system with minimum service delay and privacy preservation," ***IEEE Journal of Biomedical and Health Informatics*****, vol. 18, no. 2, pp. 430–439.**

This paper, propose an e-health monitoring system with minimum service delay and privacy preservation by exploiting geo-distributed clouds. In the system, the resource allocation scheme enables the distributed cloud servers to cooperatively assign the servers to the requested users under the load balance condition. Thus, the service delay for users is minimized.

In addition, a traffic-shaping algorithm is proposed. The traffic-shaping algorithm converts the user health data traffic to the non-health data traffic such that the capability of traffic analysis attacks is largely reduced. Through the numerical analysis, it show the efficiency of the proposed traffic-shaping algorithm in terms of service delay and privacy preservation. Furthermore, through the simulations, it demonstrates that the proposed resource allocation scheme significantly reduces the service delay compared to two other alternatives using jointly the short queue and distributed control law [4].

3. 3.EXISTING SYSTEM

Cloud computing is internet based computing which enables sharing of services. Many users place their data in the cloud. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in cloud computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. So correctness of data and security is a prime concern. This article studies the problem of ensuring the integrity and security of data storage in Cloud Computing. Security in cloud is achieved by signing the data block before sending to the cloud. Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. This paper, propose a secure cloud storage system supporting privacy-preserving public auditing. It further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Drawbacks:

- User can remotely store the data and use the on-demand high quality application and services.
- To store a data in the Cloud there is no need of local data storage and maintenance.
- Since storing large size of outsourced data, data integrity protection in Cloud computing is very challenging.
- User can resort to a Third Party Auditor (TPA) to check the integrity of outsourced data and be worry-free.
- TPA enables audits for single user.

4. PROPOSED SYSTEM

In this paper, user purchases the cloud from the cloud provider. The user will provide feedback to Cloud Provider. The new register user can access the cloud service with the permission of trust manager. The trust manager can activate and de-activate the user account. By using greedy algorithm the Sybil and collision attack will be found through the feedback and the invalid bad or malicious user is blocked. Through this feedback the reputation of the Cloud Provider will be found. If the valid user is blocked by the cloud provider the user can give the request to the cloud provider to un-block. In this paper the security for the data stored by the user is provided by using Advanced Encryption Standard (AES) Algorithm. The data stored by the user is converted into encrypted form using AES and the encrypted data is decrypted while downloading the file.

Advantages of Proposed System:

- Reputed cloud will be identified based on the user feedback.
- Good and Bad or Malicious user will be differentiated and the bad user will be blocked.
- The file will be shared in a secured manner and no one can hack the data.

User Module: User can login through the user name and password. With the permission of trust manager the can access the cloud service. The cloud consumer who use the cloud for storing the data in the cloud and the user can store the data. The user will give the feedback for the purchased cloud.

Trust Manager: The trust manager will identify the good and bad user by using the feedback provided by the user. By the use of greedy algorithm the trust manager will differentiate the attacker. The attacker differentiated by the trust manager are Sybil attack and collision attack. Through that the invalid bad user will be founded by the trust manager and the bad or malicious user will be blocked by the cloud provider.

Cloud Provider Module (Admin): Cloud provider is a super user that provides the cloud space for multiple user. The cloud provider can view all user and owner details. The cloud provider will block the bad or malicious user that are been identified by the trust manager.

Greedy Algorithm: In this paper, the greedy algorithm is used to identify the Sybil attack and collision attack from the feedback given by the user. The user who give the same e-mail id and different details for giving feedback is known as Sybil attacker. . The user who give the same name and different details for giving feedback is known as Collision attacker. Through that the bad or malicious user will be found and blocked by the cloud provider.

AES Encryption: Encrypt the portioned and conceded data. The Advanced Encryption Standard (AES) is a symmetric key block cipher published by the National Institute of Standard and Technology (NIST). Plaintext can be of 128,192 or 256 bits. Based on the bits the rounds will be generated such as 10, 12 and 14 rounds. It works under substitution and permutation principle. AES is faster.

5. CONCLUSION

The good and bad or malicious user will be differentiated by the trust manager and the bad user or malicious user will be blocked by the cloud provider. The data stored in the cloud by the user will be encrypted in a secured manner.

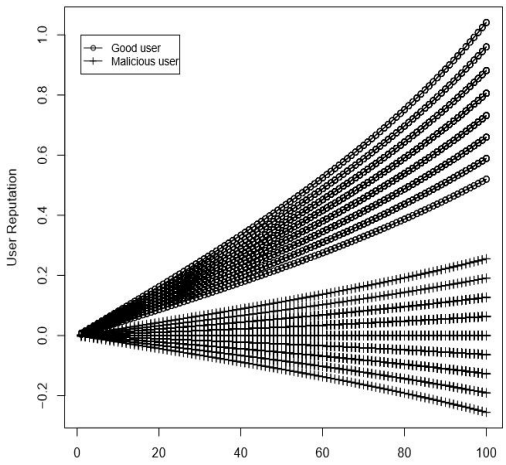

Fig. 1.It identify the number of good and bad user. Plots shows the reputation of user.

REFERENCES

[1]. Mahmoud M.M and Shen .X,(2012) "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805–1818.
http://ieeexplore.ieee.org/document/6095543/

[2] J. Huang and D. Nicol, "Trust mechanisms for cloud computing," Journal of Cloud Computing, vol. 2, no. 1, 2013.
https://journalofcloudcomputing.springeropen.com/articles/10.1186/2192-113X-2-9

[3] Y. Azar, S. Kamara, I. Menache, M. Raykova, and B. Shepard, "Colocation-resistant clouds," in Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security, ser. CCSW '14. New York, NY, USA: ACM, 2014, pp.9–20.
https://www.semanticscholar.org/paper/Co-Location-Resistant-Clouds-Azar-Kamara/7162922e14f99a005b917a4de2c28e992ecf6609

[4] Shen.Q, Liang.X, Shen.X, Lin.X, and Luo.X,(2014) "Exploiting geodistributed clouds for e-health monitoring system with minimum service delay and privacy preservation,"*IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 2, pp. 430–439.
https://www.ncbi.nlm.nih.gov/pubmed/24608048

[5] M. Macas and J. Guitart, "Trust-aware operation of providers in cloud markets," in Distributed Applications and Interoperable Systems, ser. Lecture Notes in Computer Science, K. Magoutis and P. Pietzuch, Eds. Springer Berlin Heidelberg, 2014, vol. 8460, pp. 31–37.

[6] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior,"in Proceedings of the 2Nd ACM Conference on Electronic Commerce, ser.EC'00. New York, NY, USA: ACM, 2000, pp. 150–157.

[7] S.Habib, S.Hauke, S.Ries, and M.Mhlhuser,"Trustasafacilitator in cloud computing: a survey," Journal of Cloud Computing, vol. 1, no. 1, 2012

[8] Yang .Y, Li .H, Liu.W, Yang.H, and Wen .M.(2014) "Secure dynamic searchable symmetric encryption with constant document update cost," in *Proceedings of GLOBCOM*. IEEE.

[9] Cao.A, Wang.C, Li.M, Ren.K, and Lou.W.(2014)"Privacy-preserving multikeyword ranked search over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*,vol.25,no.1,pp.222–233.
https://support.google.com/websearch/answer/173733?hl=en.

[10] Song.A, Wagner.D, and Perrig.D.(2000) "Practical techniques for searches on encrypted data," in *Proceedings of S&P*. IEEE, pp. 44–55.
[11] Yu.J, Lu.P, Zhu.G,Xue.J, and Li.M.(2013) "Towards secure multikeyword top-k retrieval over encrypted cloud data," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 239–250 .
[12] Zhang.B and Zhang.F.(2011) "An efficient public key encryption with conjunctive-subset keywords search," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 262–267.