doi: 10.30750/ijrast.549

A Review of Secure and privacy preserve data Aggregation and resource allocation in cloud computing

T.Jeyamani[1#], Dr. P. Thirumoorthy[2]*

[1#]PG Scholars, [2]* Professor,* Department of Computer Science and Engineering, *Nandha Engineering College (Autonomous), Erode, India

***Correspondence:* Dr. P. Thirumoorthy**, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode India. **E-Mail:** thiru4u@gmail.com jeyamaniit1996@gmail.com

Abstract

Cloud computing is a outstanding science that enables flexible, on-demand and low priced usage of computing resources. Cloud computing is the growing demand in recent years. However, the privacy and security threat on the stored data is major issue. The proposed work studies the security and privacy threat on data, for the applications were data aggregation is necessary. The collected data may reveal sensitive information if no security and privacy technique are applied. Thus the proposed work proved to secure by implementing techniques such as homomorphic encryption. Apart from the data aggregation and providing security and privacy to the collected data, it is important to handle the data collection effectively, for this the proposed system is enhance to provide the resource allocation. The cloud providers may have more than one cloud servers, in which the data is allocated. The problem of resource allocation will further enhance the proposed work to fulfill the needs of Cloud computing.

Keywords: Cloud Computing, Security, Privacy, Aggregation, Resource Allocation.

Introduction

Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a 'cloud'. It greatly attracts attention and interest from both academia and industry due to the profitability The cloud comprises of five essential characteristics on- demand self-service, Broad network Access, and Location Independent Resource Pooling, Rapid Elasticity and Measured service. Cloud services can be deployed in four ways based on the customers' requirements:

Public Cloud

A cloud infrastructure is provided to customers as frequent and is managed through a third party provider. Multiple corporations can work on the cloud infrastructure provided, at the identical time.

Private Cloud

Cloud infrastructure, made available only to a particular set of patron within an organization and Managed both by means of the company itself or third party service provider.

Community cloud

Infrastructure shared via several groups from identical community (Ex: Hospitals) and that will be managed via them or a third party carrier provider.

Hybrid Cloud

A composition of two or extra cloud deployment models, that transfers between them besides affecting every other.

Cloud computing can store an organization's time and money, however trusting the machine is extra important due to the fact the actual asset of any corporation is the data. Cloud computing brings a number of attributes that require specific interest when it comes to trusting the system. The have confidence of the complete gadget depends on the data safety and prevention techniques used in it. Numerous special equipment and techniques have been tested and delivered via the researchers for information protection and prevention to gain and put off the hurdle of have faith however there are nonetheless gaps which need interest and are required to be lined up by making these strategies plenty higher and effective. Owing to the giant volume of entities and get admission to factors in a cloud environment, authorization is indispensable in

assuring that solely approved entities can engage with data. By fending off the unauthorized access, agencies can achieve increased confidence in data integrity. Cloud computing vendors are depended on to hold data integrity and accuracy. However, it is imperative to construct the third party supervision mechanism besides customers and cloud service companies[1-4].

System Architecture

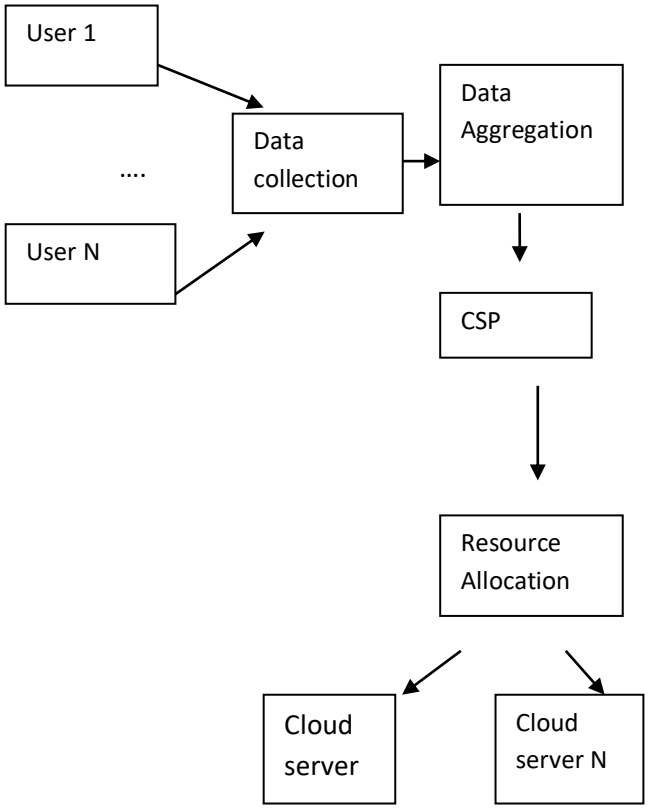

Fig 1: System Architecture

Related Works

User Shredder Module (usm)

USM will have an more privilege to interact with the Data organizer and CCSP. Whenever there is any situation for the purchaser to give up using the Cloud services. Data organizer will inform USM about the facts or content material which want to be shred in the Cloud. Then USM will engage with the CCSP and obtain get right of entry to these files and modify all the files with some random data such that no one can understand the facts reachable in Cloud and can't be used for any different purposes. Once the USM has get entry to the cloud instances, it will begin shredding all the data files by editing it with some random information in those places. This modification will be done such that, random information will no longer be associated to unique statistics in any manner. After modifying these files on Cloud, the purchaser has to leave their data on Cloud for some time to replace on all backup servers used by means of CSP to provide high availability of cloud services. As quickly as this modification has been accomplished in the Cloud via the USM, clients can start deleting their cloud instances. As the confidential statistics is no longer accessible on all of their servers. Then, purchaser can end the usage of their cloud services.

Homomorphic aggregator

This aggregator makes use of homomorphic encryption to per- shape operations in the records in a tightly closed and personal manner. To be greater precise, unpadded RSA [9] is a multiple ative homomorphic cryptosystem, while Paillier is an additive homomorphic cryptosystem. Although unpadded RSA and Paillier current interest- ing homomorphic properties, the presented case learn about here considers a method primarily based on the ElGamal cryptosystem – aggregations using other homomorphic encryptions should be performed, however. For example, Garcia et al.[10]and Erkin et al[11] .present approaches for aggregating strength consumption measurements the usage of variations of the Paillier cryptosystem.

The drawback of homomorphic aggregator is the multiplicatively homomorphic variant of RSA is not semantically secure.

Intel SGX aggregator

The Intel SGX aggregator makes use of the technology of same identify to supply safety and privacy of the sensitive information via aggregating it in blanketed areas of memory (enclaves), inaccessible even by customers with excessive privileges. In our implementation, we used the AES Galois/Counter Mode (AES-GCM) symmetric encryption algorithm described in [13] – key measurement of 128-bit – for the change of personal messages between the producers and the aggregator. In order to agree on the 128-bit key

to be used for impenetrable communication, each producer p ∈[1,n] of a subject communicates with and attests the aggregator, i.e., veri- fies that the right aggregator has been hooked up in an SGX enclave, via performing the Remote Attestation technique described in . In a nutshell, the Remote Attes- tation process leverages SGX capabilities to produce acriptographic signature of the contents of SGX enclaves and to digitally signal it the usage of a key that is solely reachable by way of the platform processor, and uses an exterior attestation carrier – currently, solely an attestation service furnished by means of Intel (IAS) can be used – to verify that the produced statistics certainly got here from the expected SGX enclave. The Remote Attestation procedure also has an underlying key change scheme based on the elliptic curve Diffie-Hellman (ECDH) key change protocol. As a result of this process, each producer will have both (i) efficiently validated the integrity of the aggregator and (ii) derived the 128-bit key kp used for tightly closed conversation – which is additionally derived via the aggregator internal the enclave. The security and privacy of the encrypted data is achieved through the guarantees pro- vided by the SGX enclaves [4].

Literature Survey

There have been lots of works done on cloud data security .The Literature survey shows that the techniques are focused on different parameters.

Improve Security over Multiple Cloud Service Providers for Resource Allocation

From the final couple of decades, computations has changed from the purchaser and server aspect to Cloud. Most of the Data generated these days is completely processed in the digital environment in contrast to the common systems. The physical place of these servers is unknown to many of the customers the usage of these services. Customers may not be conscious of the storing of their information on backup servers to supply high availability in case of any failures in one of their records centers. Users are losing full manipulate of their facts via the use of Cloud offerings compared to processing their information on private computers. What will happen to clients facts as soon as they have stopped using Cloud services? Customers statistics is definitely deleted from all Cloud servers? Even if the statistics is deleted from all of their servers, can customers will be certain their facts will no longer be reconstructed by using cloud provider issuer (CSP) the use of forensic applications? To clear up these problems, we have proposed a framework to clear up the trouble of reconstructing the data from the deleted servers the use of forensic applications[1].

Security and privacy aware data aggregation on cloud computing

The use of cloud computing has grow to be common due to advantages such as low cost and sizing of computing sources according to demand. However, it additionally raises protection and privacy worries ,because critical data–for example, in IoT applications– are stored and processed in the cloud. This paper proposes a software program architecture that helps multiple procedures to secure data aggregation. For validation purposes, this software architecture was used in the development of applications for clever grids, computing in stantaneous consumption of a place and the month-to-month invoice of an character consumer. The consumption facts can be gathered by using clever meters, enabling customers to reduce electricity cost via close monitoring. However, such data may expose sensitive records if no privateness methods are applied. Therefore, the proposed software program structure proved to be practicable from experiments with strategies such as homomorphic encryption and hardware security extensions (IntelSGX)

Cloud Computing Security Issues and Challenges

Security issues in cloud computing has performed a fundamental role in slowing down its acceptance, in reality protection ranked first as the greatest challenge trouble of cloud computing. Although Cloud computing can be viewed as a new phenomenon which is set to revolutionize the way we use the Internet, there is lots to be cautious about. There are many new applied sciences emerging at a fast rate, every with technological developments and with the doable of making human's lives easier. However, one must be very cautious to understand the security dangers and challenges posed in using these technologies. Cloud computing is no exception. In this paper key protection issues and challenges which are currently faced in the Cloud computing are highlighted [4].

Conclusion

Software requirements like security and privacy should not be ignored by applications that handle sensitive data and use cloud computing. For homomorphic encryption, the main advantage identified was the viability to implement in any environment, although it is much less efficient. Intel SGX, on the other hand,

used for the first time in a cloud computing orchestrator, yields much lower response times and allows performing various forms of computation on the sensitive data, but it demands a spe- cific infrastructure from the service provider. We presented security issues posed by using the cloud services for resource allocation from the various CSP's. It can be implemented and deployed to check the effectiveness of the framework in real time scenarios.

Acknowledgment

I am thankful for the timely and consistent cooperation given by my guide Dr.P.Thirumoorthy for preparing this survey. I hope this paper will help to understand about of Secure and privacy preserve data Aggregation and resource allocation in cloud.

References

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
2. B. Mandal, R. K. Sahoo, and S. Sethi, "Scalable big data analysis in cloud environment: A review," IJRCCT, vol. 5, no. 12, pp. 623–630, 2017.
3. .Sajjan Rajani1, Vijay Ghorpade, MadhuriDhange," Multi- factor Authentication as a Service for Cloud Data Security", International Journal of Computer Sciences and Engineering Volume-4, Special Issue-4, June 2016 E-ISSN: 2347-2693
4. VinaykumarPant ,Ashutosh Kumar , "Cloud Computing Security Issues and Challenges" , International Journal of Scientific & Engineering Research, Volume 7, Issue 6, June-2016
5. Jayachander Surbiryala, Bikash Agrawal, Chunming Rong "Improve Security over Multiple Cloud Service Providers for Resource Allocation," 2018 1st International Conference on Data Intelligence and Security
6. Barbosa M, Portela B, Scerri G, Warinschi B. Foundations of hardware-based attested computation and application to sgx. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P). Congress Center Saar, Saarbrücken: IEEE; 2016. p. 245–60.
7. Antonio, "Ddrescue - Data recovery tool." http://www.gnu.org/software/ ddrescue/ddrescue.html, 2004. [Online; accessed 31-July-2017]. Gurbinder singh brar, shalli rani, vinay chopra, rahul malhotra, houbing song energy efficient direction-based pdorp routing protocol for wsn special section on green communications and networking for 5g wireless Digital Object Identifier 10.1109/ACCESS.2016
8. M. Mihailescu and Y. M. Teo, "Dynamic resource pricing on federated clouds," in Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, pp. 513–517, IEEE Computer Society, 2010
9. Rivest RL, Adleman L, Dertouzos ML. On data banks and privacy homomorphisms. Found Secure Comput. 1978;4(11):169–80.
10. Garcia FD, Jacobs B. Privacy-Friendly Energy-Metering Via Homomorphic Encryption. In: Security and Trust Management 6th International Workshop, STM 2010. Athens: Springer; 2010. p. 226–38
11. Erkin Z, Tsudik G. Private Computation of Spatial and Temporal Power Consumption with Smart Meters. In: Proc. of the 10th Int. Conf. on Applied Cryptography and Network Security (ACNS). Singapore: ACNS 2012; 2012. p. 561–77.
12. Saroj SK, Chauhan SK, Sharma AK, Vats S. Threshold cryptography based data security in cloud computing. In: Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference On. India: IEEE; 2015. p. 202–7.
13. Dworkin MJ. Sp 800-38d. recommendation for block cipher modes of operation: Galois/counter mode (gcm) and gmac. Technical report, Gaithersburg, MD, United States; 2007.

Source of Support: Nil
Conflict of Interest: None