ISSN: 2320-1363

Enabling BlobStore for security in Cloud Storage

P. Poornima[*1], **R. Viswanathan**[*2], **I. Anette Regina**[*3]

MPhil, Research Scholar, Muthurangam Govt. Arts College, Vellore, Tamilnadu, India

Assistant Professor, Department of CS, Muthurangam Govt. Arts College, Vellore, Tamilnadu, India

Associate Professor, Department of CS, Muthurangam Govt. Arts College, Vellore, Tamilnadu, India

Abstract

The importance of strategic use of cloud services is increasing rapidly day to day . It provides the high-level direction for using cloud-based services. whereas cloud-based services share similarities with different service delivery models , they conjointly supply their own distinctive opportunities, complexities and risks. A coordinated approach is required to spot opportunities and to profit from cloud-based services. Upon choosing up the new cloud services, the essential step is to focus on low risk, low worth applications from that the organisation will live actual prices and edges, gain insights. This project deals with developing a coordinated approach to cloud-based services as an part. It shows the varied inputs that we should always take into account as they develop such an approach. we have a tendency to take appointment planning as an application and build that on a cloud platform, later it's delivered to any or all users as a Software As a Service (SaaS). so they'll customise as they have.

I.INTRODUCTION

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data.Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

One of the primary usage of cloud computing is data storage. Cloud provides enormous capacity of storagefor cloud users. It is more reliable and flexible to users to store and retrieve their data at anytime and anywhere. It is an increasingly growing technology. Nowadays, many enterprises have started using cloud storage due to its advantages. Even though the cloud continues to gain popularity in usability and attraction, the problems lie in data security, data privacy and other data protection issues. Security and privacy of data stored in the cloud are major setbacks in the field of Cloud Computing. Security and privacy are the key issues for cloud storage. This paper proposes an encryption algorithm to address the security and privacy issue in cloud storage in order to protect the data stored in the cloud.

BLOCK DIAGRAM

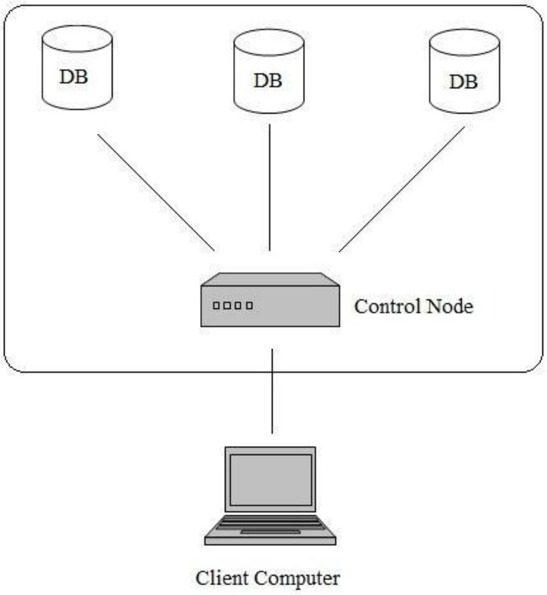

Fig 1 : A Typical Cloud Storage

Fig 1: Architecture Diagram

II.RELATED WORK

Literature survey has been done in the area of Software Engineering and its testing process.The research done by various authors are studied and some of them are discussed in the following section.

A. Enhanced Security for Cloud Storage using File Encryption

Cloud computing is a term coined to a network that offers incredible processing power, a wide array of storage space and unbelievable speed of computation. Social media channels, corporate structures and individual consumers are all switching to the magnificent world of cloud computing. The flip side to this coin is that with cloud storage emerges the security issues of confidentiality, data integrity and data availability. Since the “cloud” is a mere collection of tangible super computers spread across the world, authentication and authorization for data access is more than a necessity. Our work attempts to overcome these security threats. The proposed methodology suggests the encryption of the files to be uploaded on the cloud. The integrity and confidentiality of the data uploaded by the user is ensured doubly by not only encrypting it but also providing access to the data only on successful authentication.

B. Outsourcing and Discovering Storage Inconsistencies in Cloud through TPA

Cloud computing has changed the way computing takes place. It is the technology that enables outsourcing of computing and storage to a public cloud maintained by cloud service providers. Cloud users can use cloud storage and other facilities without capital investment in pay as you use fashion. As the data is stored in remote server in the data center of cloud service provider, there is security concern among the cloud users. Wang et al. studied this problem and ensured data integrity in cloud storage by proposing third party auditing concept. The third party auditor is responsible to verify the integrity of data on behalf of cloud data owners. The auditing mechanism

ISSN: 2320-1363

monitors the data dynamics. The solution makes use of bilinear aggregate signature for simultaneous auditing and Merkle Hash Tree for secure block level authentication. In this paper we implement a prototype, Java custom simulator, which implements the proof of concept proposed by Wang et al. The empirical results revealed that the prototype is effective to demonstrate the efficiency of auditing mechanism to ensure data integrity.

C. QoS Aggregation for Web Security service composition Using Workflow Patterns

Web Security service composition uses the non-functional characteristics having some criteria for finding and selecting available services. This paper focuses on overall Quality of Service (QoS) of a composition by aggregating the QoS of the individual services. It verified whether a set of services satisfies the QoS requirements for the whole composition or not. Mainly, the aggregation performed builds upon abstract composition patterns, which model basic structural elements of a composition like parallel paths, a sequence, or a looped execution. Here, 2 issues are there. First, in conditional branches the actual distribution is needed about how many times the individual services are picked. But the services are often chosen differently during runtime so the mean execution time depends on their distribution. Second, while the minimal or maximal execution time for individual services can be advertised in advance by the provider, the mean execution time of a service depends on the concrete invocation. Since the execution time is depend on the complexity of the input data. Thus, calculation of the mean execution time must include measurements during runtime to give a closer approximation of the delivered QoS.

Also, it explains about workflow patterns which helps to form a set of composition patterns to realize an approach for the aggregation of QoS. It explains the composition patterns, aggregation with dependency, monitoring the composition. But QoS Aggregation in WSC does not give reliability when user triggering the Services. It has restricted to predefined workflow so lack of guarantee for getting the optimal QoS value

III PROBLEM DEFINITON AND METHODOLOGY

PROBLEM IDENTIFICATION

Cloud storage enables the users to access the data anywhere across the globe. The data integrity and data security is considered to be the key area of research in cloud computing. In this thesis, we deal with the data security issues which is being faced in cloud computing. The problem is identified considering the issues faced by many users across many places. The cloud attacks leads to loss of confidential data which is stored in the cloud servers. In order to solve this problem, the cloud security is implemented using blob store in this paper.

PROBLEM DEFINITION

As the importance of cloud increases day to day, the technology face different security issues on maintaining data integrity. The data inconsistency and data deduplication issues plays a vital role in cloud computing challenges. The data uploaded from the client end needs one more layer of security where the data is binded with the encryption key. In this project, the concept of blobstore is used secure the data in to blob keys

PROBLEM DESCRIPTION

The blobstore is implemented using a WSC provides an open, standards-based approach for connecting web services together to create higher-level business processes. The Semantic Web community focuses on reasoning about web resources by explicitly declaring their preconditions and effects with terms precisely defined in ontologies. In automated Web Security service composition, workflow is the main process which invoke application or external services and/or assigning manual task in automated manner.

Some problems exist during these process such as the number of web services is increasing with time and it is difficult to search the whole repository for desired service in order to use it for the fulfillment of specific goal. These process has to be overcome by applying planning based approach. It is achieved by applying the CORS mechanism which allow many resources such fonts, JavaScript etc., on a web page to be requested from another domain outside the domain from which the resource is originated. Also we use the technique called JSONP for cross domain requests.

To make the cross domain resource sharing, it is used. In order to make a cross domain call efficiently and fastly, HTTP Redirect is used to make a cross domain call to the third party service where it automatically redirects the reader's browser to a specified target space.

For high reliability, additionally OAuth2.0 is enforced for authorization. It is a way to publish and interact with protected data. Once the request is successful, channel API used for multiuser chat among other channels. Approximation Algorithm used to reduce the time complexity for getting optimal QoS value.

III.EXISTING SYSTEM

Cloud security and privacy concerns are arising in which both customer's data and application are residing in provider's premises. While cost and ease of use are two great benefits of cloud computing, there are significant security concerns that need to be addressed while moving critical applications and sensitive data to public and Cloud storage. Cloud data may be attacked in two ways. One is outsider attack and the other is insider attack. Insider as an administrator can have the possibility to hack the user‟ s data. Insider attack is very difficult to be identified. So the users should be very careful while storing their data in cloud storage. Cryptography is a technique applied for encryption and decryption. In the field of cryptography there are several techniques available for encryption/decryption. These techniques can be generally classified into two major groups, i.e. Conventional and public key Cryptography. In public key cryptography, the plain text is converted to cipher text to protect the data secured from hackers and intruders.

Web Service applications is the main method to efficiently and effectively select and integrate inter-organizational and heterogeneous services on the web at runtime. WSC transforms a composition task with multiple global QoS constraints and preferences to a planning problem with temporal and numeric features. Here, QoS-Aware WSC describes Local optimization, Integer programming models. Planning based WSC approach solves cost sensitive temporally expressive (CSTE) planning problem by SAT-based cost planning (SCP) solver. Additionally,Q-WSC problems that is numeric planning problem can be solved by metric-based planner Metric- FF to obtain the QoS value.

IV DISADVANTAGES OF EXISTING SYSTEM

- Security threat in storing public key. In case of exposing the key, the data could be easily decrypted and stolen,
- No remote access for the data.
- It degrades the efficiency and reliability of QoS and does not provide non-functional properties accurately when user selecting the web services.

- Web Security service composition method does not provide the optimal QoS value when using numerical temporal planning.
- For large instances, this process does not solve easily to obtain the value.
- By using Local optimization and Integer programming, the global QoS constraints cannot achieved more.
- It increases Computational cost and time for a composition task

Latency is encrypting huge size of files.

IV.PROPOSED SYSTEM

Storing BLOB data such as images, audio files, and executable files in the database with typical text and numeric data lets you keep all related information for a given database entity together. Blobstore enables easy search and retrieval of the BLOB data by simply querying its related text information. However, storing BLOB data can dramatically increase the size of your databases.

The common alternative to this technique is storing binary files outside the database, then including as data in the database a file path or URL to the object. This separate storage method has a couple of advantages over integrating BLOB data within the database. It's somewhat faster because reading data from the file system involves a bit less overhead than reading data from a database. And without the BLOBs, the databases tend to be smaller. However, the link must be manually created and maintained between the database and external file system files, which have the potential to get out of sync. In Blobstore, the data is stored in a highly secured manner which uses the blob key to represent the file.

Web Security service composition is the task of combining a set of single web services together to create a more complex services. The proposed system used to make a cross domain call among web services by a Cross Origin Resource Sharing (CORS) which allows many resources from outside domain where the browser and the server are interact to determine whether or not to allow the cross-origin request. It is related to JSONP technique to achieve the cross domain requests. Also, predefined workflow and planning based approach method is enhanced which uses HTTP Redirect concept to make a cross domain call to the third party service.

Additionally, exactDestination and httpResponseStatusattributes allow you to configure the end-user experience of the redirection. Using this prototype, Open Authentication protocol 2.0 is used to make the cross domain call and once the request is successful, Channel API is used. In this paper, channel API based multiuser chat is implemented to show the efficiency of web service call made on every chat which is exhibited using many different channels. This will update the information to users quickly. To minimize the computational time, an approximation algorithm is used.

V. CONCLUSION AND FUTURE ENHANCEMENT

Cloud computing is an emerging technology which provides lots of benefits to the user. It reduces the maintainance cost and the resource cost for the clients who requires cloud service. As seen on the above contents, Cloud computing incurs a lot of security issues, especially in terms of large file storage. In order to avoid the attacks and threats happening to the cloud storage, the concept of BLOB STORE is used in this paper to address the threats. Cloud computing supports an enormous fast and lighting speed technology, a huge array of applications to use, seemingly unlimited storage space. The security threats which emerge with shared spaces such as breach of confidentiality, hampering of data integrity and non-availability of data is discussed in this paper. In this paper, we have proposed a framework which encrypts a file before it is uploaded on to the cloud. BASE 64 is one of the most secure encryptedformat and not many attacks are successful on data which is encrypted using BASE 64 encoding. This proposal solves the problem of most, if not all, of the threats that data stored in the cloud faces. Our framework also suggests the use of login id and password to ensure authentic and authorized access to a user's data. Thus, if used securely, cloud computing provides a user with amazing benefits and overcomes its only disadvantage of security threat.

The Proposed Framework can be developed in the form of Mobile application using various operating systems such as Andriod, iOS, Blackberry. It can also be merged with social networking sites, to exchange the data securely and safely in a encrypted form. The algorithm can also be enhanced to not only encrypt text files, but also video and audio files. The image file is already being supported by the proposed framework.

REFERENCES

1. J. Rao and X. Su, "A Survey of Automated Web Security service composition Methods," Proc. First Int'l Conf. Semantic Web Servicesand Web Process Composition, vol. 3387, pp. 43-54, 2005.

2.J. Haddad, M. Manouvrier, and M. Rukoz, "TQoS: Transactional and QoS-Aware Selection Algorithm for Automatic Web Security service composition," IEEE Trans. Services Computing, vol. 3, no. 4, pp. 7385,Jan.-Mar. 2010.

3.S. Sohrabi and S. McIlraith, "Preference-Based Web Security service composition: A Middle Ground between Execution and Search,"Proc.

Int'l Semantic Web Conf. (ISWC '10), 2010.

4. D.A. Menasce´, "Composing Web Services: A QoS View," IEEEInternet Computing, vol. 8, no. 6, pp. 88-90, Nov./Dec. 2004.

5.M. Jaeger, G. Rojec-Goldmann, and G. Mu´hl, "QoSAggregationfor WebSecurity service composition Using Workflow Patterns," Proc.Int'l Enterprise Distributed Object Computing Conf., 2004.

6. Shuiguang Deng, Longtao Huang, Wei Tan, Senior Member, IEEE, and Zhaohui Wu, Member,IEEE"Top- k Automatic Security service composition: A ParallelMethod for Large-Scale Service Sets", IEEE Transactions on Automation Science and Engineering, vol. 11, no. 3, july 2014

7.S. Hwang et al., "Dynamic Web Service Selection for Reliable WebSecurity service composition," IEEE Trans. Services Computing, vol. 1,no. 2, pp. 104-116, Jan. 2008.

8. S. Sohrabi, N. Prokoshyna, and S. McIlraith, "Web Security service composition via Generic Procedures and Customizing UserPreferences," Proc. Int'l Semantic Web Conf. (ISWC '06), 2006.

9. Yang Yu, Jian Chen, Shangquan Lin and Ying Wang, "A Dynamic QoS-Aware Logistics Security service composition Algorithm Based on Social Network," IEEE Transactions on Emerging Topics in Computing,DOI 10.1109/TETC.2014.2316524,

10.Guoping Zhang, Wentao Gong , Jiazheng Tian, "The Research of Cross-Domain Usage Control Model in Web Services," e-Business and Information System Security (EBISS), 2010 2nd International Conference on May 2010.