A MULTI-SERVER DATA SECURITY WITH PUBLIC AUDITING IN CLOUD COMPUTING

Dinesh R1, Ezra Vivin A2
U.G Student, Department of Computer Science & Engineering
Sathyabama Institute of Science and Technology, Chennai, India
1rjdinesh4@gmail.com, 2vivinezra@gmail.com

Dr. Srinivasan N3
Professor, Department of Computer Science & Engineering
Sathyabama Institute of Science and Technology, Chennai, India
3professorsrini@gmail.com

Albert Mayan J4
Assistant Professor, Department of Computer Science & Engineering
Sathyabama Institute of Science and Technology, Chennai, India
4albertmayan@gmail.com

Abstract: In cloud computing, user share data while sharing data providing security and protecting the data from unauthorized users is still a demanding problem, so we implement a multilevel data security popular a cloud computing in order to preserve the information using multi-security levels, and provide sufficient multilevel access and validate authorized identity. The recommended scheme is dynamic in multilevel data security, adaptable to certified resource share in, and protected against different malignant strike. Experimentation result checks the feasibleness. The processed data have multiple security level and access permission.

Keywords: Third Party Auditor, Authentication, Access control, Transparent Computing, Data Security.

1. INTRODUCTION

Over few years, computing has a great development in emerging technologies. Transparent computing is a development technology which helps the user to access user-controlled services. It carries a different variety of heterogeneous OS's and application dynamically in different devices. It allows the user to focus on the available services without depends upon the substantial devices that will be used and depends on which disk should be operated.

The new process comes with the advantages in multiple security aspect. This security system make the user data secure, lowers the theft and reduces the risk of data leaking using centralized management in server side. But still, challenging problem in providing security in different OS's and integrate between data application in servers are shared in cloud computing. The data has a different level of the security system and for example: Consider enterprises which introduce transparent computing as its system. In this module (e.g. data files and information) will be used as their daily activities for updating the information of the employee in the enterprises According to data security, common information can be shared with all public user whereas the sensitive information is been encrypted form only the Data Owners has permission to give the user to access the information. The user can access
the protected files which have been encrypted by the owner, the owners give the access permission using a special key to some specific users. But third users cannot access the protected file which is encrypted by the owner. The authorized owner only has the access update, append and delete the files/information which he wants to perform. Without the knowledge of the user, the data might be misused or embezzled by unauthorized access users. So this process is engaged to encrypt the private source of all users before stored the data in transparent servers. A multilevel security is implemented to protect the user information and provide exact access control to them. The precise scheme which was used to multilevel confidently and fine-grained access was Attribute-Based Encryption (ABE) but it, consumes more expensive due to bilinear map operation. Additionally, if the user revocation process is an unmanageable problem, so it should be processed to get data re-encrypted. We introduce an authentication server to perform identity authentication and multilevel access control with the user level data access, storage transversal in transparent computing.

2 RELATED WORKS

We have Liu et al proposed a financially savvy unwavering quality administration instrument POCR in light of a summed up information dependability demonstrate. It instate the information dependability while information requires least number of copy duplicate.

C. Wang et al (2013) proposed a protection safeguarding in broad daylight reviewing framework for information stockpiling security in distributed computing. It utilize direct reviewer and arbitrary concealing to acknowledge that TPA will recognize the server amid the procedure. This procedure is done for numerous clients for different data. So protection assurance is gotten to from numerous client security in distributed computing.

J. Kar2012 proposed "a provably secure on the web/disconnected total mark conspire in irregular prophet model" and this plan can be actualized on low processor gadgets, for example, savvy card, PDA and so on and WSNs applications. This scheme is based on identity-based signature using scour. It is used to detect the unauthorized user with no identity and in order to protect their content from the third party.

H. Jin et al in this paper, the data auditing of the web content based on their paper content and the title of the paper. we need to evaluate both content page and title to be related on the time of data evaluation to find the mismatched content. If any mismatched will find the server needs to give some alert messages to client system while the time of data uploaded on to the server. For these evaluations, we are using some arbitration protocol to finds the mismatched content on the web pages.

S. g. work et al proposed to give a cryptanalysis in Work et al's. Conspire and demonstrate their plan has a security blemish. Misusing the security imperfection, a foe can discretionarily alter the cloud client's information while keeping away from the discovery. The formal security verification and execution investigation show that our plan is secure and as productive as work et al's. Plotted Security and performance analysis demonstrate that our scheme is secure and as efficient as work et al.'s schemed Security

J. Yu, K. Ren, C. Wang, and V. Varadharajan 2015 proposed in that existed framework they are utilizing some multi-catchphrase pursuit to discover the client sought information. For that, they are taking the papers from the historical backdrop of hunt to effectively get the client intriguing data. The issue we have to process with a bigger measure of information. That is the reason we are executing our advantage models for each and every client with the assistance of semantic cosmology WorldNet to understand the client's need. To take care of the issue to take quite a while information handling.

3 PROPOSED SYSTEM

We utilize different security courses with a specific end goal to shield the information from third client different noxious assault. This plan is managed multilevel control in straightforward registering and it comprises of three gatherings: the client/translucent customer (TC), the verification server (AS) and the translucent Server (TS). In these, we start the client and straightforward customer as one section after the joined check between Authentication servers (AS), the Third Party Auditor (TPA), which is arranged amongst Tc and Ts.
The main purpose of the authentication server is to verify the authorized individual and to check the read and write access permission to protect the data. Public information can be shared to all users, whereas the private/protected data are encrypted by the owner to protect the information from the revoked user. In order to view encrypted information, the third user requests a token to the owner, and the owners respond to the specific user with the valid key. We distribute files/information into segments in order to provide fast and secure access transmission. The client can part the data either out in the open or ensured shape. Blunder location strategy to check whether the data gave by the client is applicable or not. The strategy utilized hub side level line mistake, edge side level line, hub side information lost blunder, edge information lost blunder, hub side too far out mistake, edge side beyond the field of play mistake, hub side spike mistake and edge side spike mistake.

4 TECHNIQUES PRELIMINARIES

4.1 MODULES

4.1.1 Administrator
The administrator can view the new user details and give access to the user to upload the file in cloud storage. It can view all user details and the uploaded files.
User details and file details: The administrator views all user and file details. It can see the number of individual uploaded files. It creates a report based on uploaded file.

4.1.2 Data Owner

New user: In this module, the administrator can view all new user details. It authorizes the new user to upload files. If the authorization is not processed by the admin, the process cannot be processed.

User phase:
In client stage, the new client moves to the login page where the client should enter the client name and secret word. The client gets a security enter with a specific end goal to process to the document transfer or download page.

4.1.3 File upload

The user module consists of file upload. In this module, the user can upload the file. While uploading, the user should share the secret key. The secret key and the file are positioned in encrypted form.
4.1.4 File upload and append

If user want to download the file, the user must give the secret key. On the off chance that the client gives the right mystery key while downloading, the first record will be downloaded else the encoded document will be downloaded. On the off chance that the client needs to erase his transferred document, the client must give the mystery key else the client can't erase the client record.

4.1.5 Authenticator Server Module

The main aim of the server is to be part of both user and cloud server. The server checks the valid user using a private key and if the key matches then he/she can access the check process to store the relevant information in the cloud storage. The server checks the information sent by the user is a valid information.

4.1.6 Error Detection

Cloud computing is an emerging technology which has vast improvement because it provides open, flexible, scalable, reconfigurable platform. The proposed error detection will be based on the nine types of numerical data abnormality/error are listed in our cloud error detection approach. The error detection process is trigger by defined error model. The contribution of our proposed detection is to achieve performance improvement in error detection without compromising.
4.2 Algorithm

4.2.1 K-segmentation algorithm:

In segmentation algorithm, an example for describing this process we use dynamic programming. Firstly, let us consider a set of ‘n’ data points where data cannot be executed by least squares regression technique which is not possible by a single line data. Rather, we use the model for default line segments. To be more specific, we implement piece-wise regression for segmentation where \((1 \leq k)\) and \((k \leq n)\) of \(n\) points. The least square techniques were repudiated because if \((k=1)\), two degree of freedom is the best choice than one degree of freedom, and \((k=n)\) does not fit the point as single line segments are retrieved for every single point.

Actually, the problem can be defined as:

Consider a set of \(n\) data points \((x_1, x_2, \ldots, x_n)\) where a piecewise sequence is assigned to generate a line segment \(l_{sj}\) where \((j=1, k)\)with \(l_{sj}=(s_j, e_j, p_j)\). the line segment \(l_{sj}\) case the expression initialize with \(x_{s_j}\) and end with \(x_{e_j}\). The overall standard of the fit is analyzed by reducing the total fit error.

\[ E_s = \sum_{i=1}^{n} w_i (x_i - x_j)^2 \]

Where \(x_j = b_j\) for \(s_j \leq i \leq e_j\) and \(w_i\) is a measuring factor for each points.

4.2.2 Indexing and Merging Algorithm:

Indexing, an additional structure that accepts inverted list to access it randomly. In the part of merging techniques, there is a decrease in the requirement of disk space. Adding to it, the inverted list specify alternation of the structure and which is more significant for the collections of a vital document. We enhance merging techniques which are required to evaluate the data structure and the performance improvement. The inverted list that contains an entry for every works that which are in the stored document which consists of the document number and position information. It enables run length encoding and one pass compression techniques for better search and storage requirement. We implement an index structure as same as B-tree for the long list.

Run-length encoding and compression with a tree do not compress more space than a sequential list. The number of document starting from leaf node run-length. Dead spaceman leaf node terms document number. In every node, dead space should be represented. Unnecessary traversing of the tree should be eliminated. This technique implies that the area of the death of child node where the information stored in every non-leaf node,

\{ \text{Min, Max, ds; ref} \}

Where min and max is the minimum and a maximum number of subtree sourced by the ref, and ds is the dead space of the children node. The dead space is that the sum of the length extends from the node is not of the child node.
int sizeRemaining = (int)fiSource.Length;
for (int i = 0; i < OutputFiles; i++)
{
    currPartPath = FolderOutputPath + "," + fiSource.Name + "." + String.Format("{0:D4}", i) + ".txt";
    if (!File.Exists(currPartPath))
    {
        fsPart = new FileStream(currPartPath, FileMode.CreateNew);
        sizeRemaining = (int)fiSource.Length - (i * partSize);
        if (sizeRemaining < partSize)
            partSize = sizeRemaining;
        fsPart.Write(byteSource, fileOffset, partSize);
    }
}

Randomval = new Random();
int rno = val.Next(12345, 54321);
cryptographykey = Convert.ToString(rno);
fileenccryptographykey = cr.Encrypt(cryptographykey);
splitfilesize = Convert.ToString(filesiz);
GenToken();
Label16.Text = tocken;
Image6.ImageUrl = "Images/allowicon.png";
TextBox3.Text = cr.Decrypt(TextBox3.Text);
TextBox3.ForeColor = System.Drawing.ColorTranslator.FromHtml("#000000");

5 CONCLUSION

We enhance a method called multilevel access control in the transparent computing scheme to preserve user data with multiple security level. The main objectives maximum security for multi-data access, storage and processing in transparent computing also time efficient theme for locating and detecting error. In future works, we will enhance by initializing multiple authenticator server (AS) to resist traffic between the users (TS) and the server and to detect issues like error correction and recovery in cloud computing and to ensure the high accessibility of the system.

REFERENCES

1. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy preserving public auditing for secure cloud storage,” IEEE Transactions on Computers 2013.
2. Albert Mayan.J, Surya.B, Pranoy Prabhakar, Prince kumar,” Department–Student Library Using Twig Pattern Query Processing Over Admin–User Login Privilege”, Pak. J. Biotechnol. Vol. 13 , Pp. 489 - 493,(2016).
3. D. He, S. Zeadally, and L. Wu, “Certificateless public auditing scheme for cloud-assisted wireless body area networks,” IEEE Systems Journal, pp. 1–10, 2015.
4. Surya.V, J. Albert Mayan,” A Secure Data Sharing Mechanism In Dynamic Cloud By Using KP-ABE", Research Journal of Pharmacy and Technology , Vol 10 , Issue 1 , pp:83-86,2017
5. H. Jin, H. Jiang, and K. Zhou, “Dynamic and public auditing with fair arbitration for cloud data,” IEEE Transactions on Cloud Computing 2016.

6. Lakshmanan, L. and Shankar, (2015), “Dynamic cognitive system for recovering from vulnerable attacks in social network”, International journal of Applied Engineering Research, RIP India, Vol. 10, No.4, pp.10365-10374, India, 2015, ISSN: 1087--1090.

7. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy preserving public auditing for secure cloud storage,” IEEE Transactions on Computers, vol. 2009.

8. Y. Zhang and Y. Zhou, “Transparent Computing: Spatio-temporal Extension on Von Neumann Architecture for Cloud Services,” Tsinghua Science and Technology, vol. 18, no. 1, 2013, pp. 10–21

9. Y. Zhang and Y. Zhou, “Transparent Computing: a New Paradigm for Pervasive Computing,” Ubiquitous Intelligence and Computing:2006 International Conf.(UIC 06), 2006, pp. 1–11

10. G. Wang, Q. Liu, J. Wu, and M. Guo, “Hierarchical Attribute-based Encryption and Scalable User Revocation for Sharing Data in Cloud Servers,” Computers & Security, vol. 30, no. 5, 2011, pp. 320–331.

11. Yovan Felix A, Jesudoss A, Albert Mayan J (2017), "Entry and exit monitoring using license plate recognition ", IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), pp.227-231.

12. Q. Liu, G. Wang, and J. Wu, “Time-based Proxy Re-encryption Scheme for Secure Data Sharing in a Cloud Environment,” Information Sciences, vol. 258,2014, pp. 355–370.

13. Jabez J, Gowri S, Vigneshwari S, Albert Mayan J and Srinivasulu S (2018)," Anomaly Detection by Using CFS Subset and Neural Network with WEKA Tools", Smart Innovation, Systems and Technologies,Vol.107, pp. 675–682.

14. Kamalesh M. D., Albert Mayan J, Felix Y., Sumanth B. S., & Sai Tej B. (2018), " Magrisys: A Smart And Ubiquitous Controlled – Environment Agriculture System " , 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) , pp: 1-5 , 2018

15. S. Muruganandam , N. Srinivasan ,"Appraisal of Felder - Silverman Learning Style Model with Discrete Data Sets",Indian Journal of Science and Technology, Vol 9(10), DOI: 10.17485/ijst/2016/v9i10/88992, 2016