MJRET

Open Access

Multidisciplinary Journal of Research in Engineering and Technology

Journal homepage: www.mjret.in

ISSN:2348 - 6953

DATA SHARING MANAGEMENT IN TRANSPARENT COMPUTING

Shashank Bapure, Shubham Mate, Pankaj Patil,

Shubham Poman, Laxmi Madhuri

Computer Engineering, Dr D Y Patil School of Engineering,

Lohegaon Pune, India

Abstract: *The transparent computing is gaining more and more courtesy in recent times. Resources are stored on remote servers, and delivered on demand to clients in a streaming way. The centralized management at servers can bring convenience security for user's information. This approach is greatly useful to protect the user data with different security levels, and provide multilevel access control and valid identity authentication. The proposed scheme is effective in multilevel data security, flexible in authorized resource sharing. Scope of Transparent Computing is enormous and wide spread, which can be used in almost all the information technology domains. By asymmetric group key agreement and group signature, propose an efficient data auditing scheme for to check the file Integrity while at the same time providing some new features, such as traceability and countability.*

Keywords: *Access control, Transparent computing, Authentication, Computer security Multilevel security, Access control, Privacy.*

1. INTRODUCTION

Transparent computing is the new emerging technology, which helps users to enjoy user-controlled services by extending the stored program concept. Transparent computing loads a various heterogeneous OSs and applications dynamically on different device. This feature enables users to keep a eye on the available application services without caring about which physical device will be used and what OS should be run on it. The new concept comes with many advantages in information security aspect. In the centralized management at the server side have a security related many advantages. By using this type of security the user

data makes a secure, and also lowers the risk of data theft and the risks of information leakage. But it is challenging in provide a security in the different Oss, data and applications are centralized in serves are shared by different users in transparent computing system.

Provide three types of users. Public users which are can gain access to files which are public files. These are encrypted by the owner and give permission to the all users. The user can access the file that has a encrypted by the owner and give access to the specific users &third user in this the file is encrypted by owner and could not give access permission to the any user. Only the owner can get access to file and performs read, write what he/she wants to perform. In this AS is the main part. This is going to authenticate the user. And also checks the permission of user related to the file. The AS can validate the user by using a username and password.

2. LITERATURE SURVEY

A Multilevel Access Control Scheme for Data Security in Transparent Computing [1]:

In transparent computing, the client terminals are rather light-weighted, while all of the resources (including the operating systems, OSs for short) are stored on remote servers, and delivered on demand to clients in a streaming way.

Spatio-temporal Extension on Von Neumann Architecture for Services, Tsinghua Science and Technology [2]:

With the rapid improvements in hardware, software and networks, the computing paradigm has also shifted from mainframe computing to ubiquitous or pervasive computing, in which users can get their desired services anytime, anywhere and any means. However, the emergence of ubiquitous or pervasive computing has brought many challenges, one of which is that it is hard to allow users to freely obtain desired services, such as heterogeneous OSes and applications via different light-weight embedded devices. We have proposed a new paradigm by extending the von Neumann architecture spatio-temporally, called Transparent Computing, to store and manage the commodity programs including OS codes centrally, while streaming them to be run in non-state clients. This leads to a service-centric computing environment, in which users can select the desired services on demand, without concerning these services' administrations, such as their installation, maintenance, management, upgrade, and so on.

Transparent Computing: a New Paradigm for Pervasive Computing, Ubiquitous Intelligence and Compuing [3]:

Cloud computing has become a hot topic recently. Among these research issues, cloud operating systems have attracted extensive attention. However, to date, there is no answer

to such issues as what a cloud operating system is and how to develop one. This paper proposes a cloud operating system, TransOS, from the viewpoint of transparent computing, in which all traditional operating system codes and applications are centrally stored on network servers, and an almost bare terminal dynamically schedules the necessary codes selected by users from the network server, and runs them mostly with the terminal's local resources. The TransOS manages all the resources to provide integrated services for users, including traditional operating systems. This paper first introduces the concept of transparent computing as a background and presents TransOS and its main characteristics. It then gives a layered structure-based designation of TransOS and finally illustrates one example of its implementation.

TransOS: a Transparent Computing-based Operating System for the Cloud, International Journal of Cloud Computing [4]:

Proposes a cloud operating system, TransOS, from the viewpoint of transparent computing, in which all traditional operating system codes and applications are centrally stored on network servers, and an almost bare terminal dynamically schedules the necessary codes selected by users from the network server, and runs them mostly with the terminal's local resources. The TransOS manages all the resources to provide integrated services for users, including traditional operating systems.

3. PROPOSED SCHEME

Aim to build a prototype system which is shown in Figure, which is used for authenticate the user and provide a Multi Level security to the files for reading, writing and updating in transparent computing. With Public Auditing on the server regarding client access information that Increase the user Efficiency.

User : The user is registered first. After that the user is login into the system. The Authentication of the user at login time is performed by the authentication server. Once the login success then user will upload the encrypted files and also make a request for file. And get the requested file along with decryption key. Also we send the decryption key of file on user mail and opt also used for Authentication Purpose.

Authentication Server: It is performed the authentication of the user. It is also checks the permission of the user related to the file. After it forwards the request to transparent Server. And the History Of all data user is maintained.

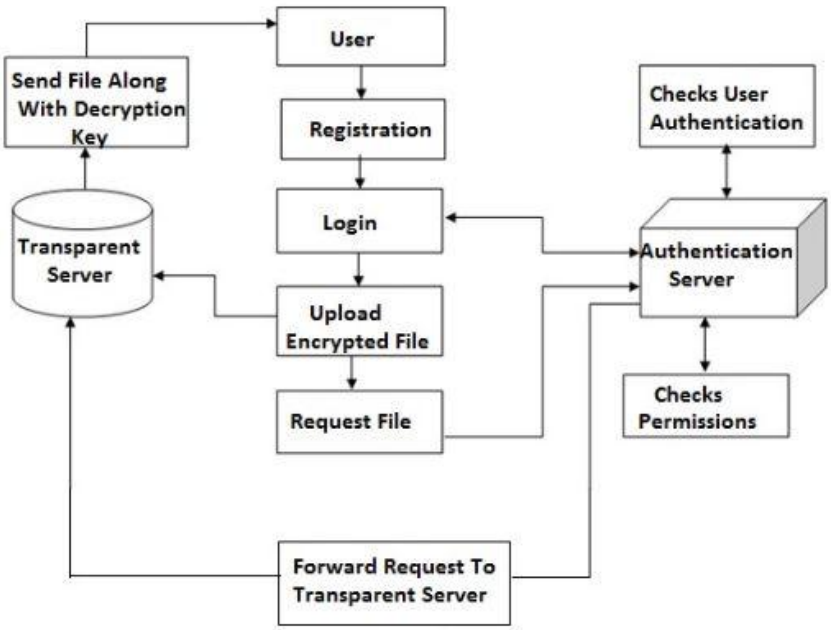

Fig 1. System Diagram

Transparent Server: It sends the requested file along with decryption key to the user.

Modules:

1. User Registration (Sign In / Sign Up)

2. Uploading Files

3. File Preview and Downloading

User Registration: In this module first user register with our application by adding his personal information like his name, password, address and his hobbies etc. After registering with our application he can login with us using userid and password. System authenticate this information and allows user to login into the system.

Uploading Files: After login, the user can upload the files to the cloud server space. The Uploaded files are getting separated in to multiple parts and those parts are getting encrypted using the ECC algorithm. Here the Working of Merkle Hash tree starts. The Leaf nodes of the Merkle Hash Tree will be the File Parts.

File Preview and Downloading: After file Uploading has been done user can Update and Preview the File. The user can Directly access the specified part for the updating. The Updating will be done in that specific part instead of the Whole file. The is the fine grained updates. For each operation like Preview and Updates the files are getting Decrypted , Encrypted and Merge for each operation.

Algorithm :

ECC : The ECC Algorithm is public key encryption technique which dependson *elliptic curve theory*.In Elliptical curve cryptography key generation takes place through the properties of the elliptic curve equation instead of using the traditional method of generation as taking the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods.

1.select the file type then select plain text from the file

2.After selecting file select the output file

3.After selecting output file check if file compress or not

4.if the file compress then check the plain text is converted to ciphertext or not(encrypted file)

5.if text in file are hidden or converted to ciphertext then encryption is successful.

6.for retrieving encrypted, hidden, compressed message select the output file for retrieving output file enter key or password.

Key generation steps:

Parameters (q, FR, a, b, G, n, h).

1. Select random number p, p∈ [1, n – 1]
2. Compare K = pG.
3. public key is K and private key is p.

A public key K = (vq, wq) associated with the domain parameters (q, FR, a, b, G, n, h) is validated using the following procedure

1. Check that K ≠ O
2. Check that vq and wq are properly represented elements of Fq
3. Check if K lies on the elliptic curve defined by a and b.
4. Check that nK = O

SHA1: Secure Hash Algorithm it is used for the Public Auditing of file to check the integrity.

4. CONCLUSION

Proposed system have implemented multilevel security for the access to the files. The owner of the file gives access permission to the users. The proposed scheme is effective in multilevel data security, flexible in authorized resource sharing Public Auditing, and now days Scope of Transparent Computing is enormous and wide spread, whichcan be used in almost all the information technology domains.

In Future you can used more Secure Algorithm and authentications Method that Can increase the multilevel security, access control, Public auditing and all.

ACKNOWLEDGMENTS

We would like to heartily acknowledge all the group members who put their heart and soul in it to make it a successful project. We would like to thank our guide Ms. Laxmi Madhuri for guiding us on every possible juncture while making the project. It is due to his very crucial critics that molded the project into its finished form also a lot of thanks to all the near and dear ones who helped us with whatever small contributions that made this project possible.

REFERENCES

[1]. A Multilevel Access Control Scheme for Data Security in Transparent Computing, 2016 IEEE.

[2]. Y. Zhang and Y. Zhou, Transparent Computing: Spatio-temporal Extension on Von Neumann Architecture for Services, Tsinghua Science and Technology, vol. 18, no. 1, 2013, pp. 1021.

[3]. Y. Zhang and Y. Zhou, Transparent Computing: a New Paradigm for Pervasive Computing, Ubiquitous Intelligence and Computing:2006 International Conf. (UIC 06), 2006, pp. 111.

[4]. Y. Zhang and Y. Zhou, TransOS: a Transparent Computing-based Operating System for the Cloud, International Journal of Cloud Computing, vol. 1, no. 4, 2012, pp. 287301.

[5]. Y. Zhang, L. T. Yang, Y. Zhou, and W. Kuang, Information Security Underlying Transparent Computing: Impacts, Visions and Challenges,Web Intelligenceand Agent Systems, vol. 8, no. 2, 2010, pp. 203217.

[6]. G. Wang, Q. Liu, Y. Xiang, and J. Chen, Security from the Transparent Computing Aspect, Pro. 2014 IEEE Conf. Computing, Networking and Communications (ICNC), 2014, pp. 216220.

[7]. 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. 355370.

[8]. G. Wang, Q. Liu, J. Wu, and M. Guo, Hierarchical Attribute-based Encryption and Scalable User Revocation for Sharing Data in Cloud Servers, Computers and Security, vol. 30, no. 5, 2011, pp 320331.

[9]. Y. Zhang and Y. Zhou, 4VP: a Novel Meta OS Approach for Streaming Programs in Ubiquitous Computing, Advanced Information Networking and Applications: 21st International Conf. (AINA 07), 2007, pp. 394 403.

[10]. *H.-A. Park, J. W. Hong, J. H. Park, J. Zhan, and D. H. Lee, Combined Authentication-based Multilevel Access Control in Mobile Application for Daily life service, IEEE Transactions on Mobile Computing, vol. 9, no. 6, 2010, pp. 824837.*