JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A framework on Group Data sharing based agreement implementation in cloud computing

[1]Ms. Sohilara Kazi, 2Dr. A. S. Kapse,

[1]Student, CSE Department, Student, Anuradha Engineering College, Chikhli, INDIA
[2]Associate Prof., HOD, CSE Department, Asst. Prof., Anuradha Engineering College, Chikhli, INDIA

Abstract : The main process includes inputting the dongle after the computer is running and then verifying the media. If the conditions are met, the media will be further loaded, and if the media verification is not passed, the program will be forbidden. At this time, the entire system cannot continue to run, and the judgment efficiency is high. After the loading medium is passed, the next step is to verify the certificate file and then verify the user' name and password. After these subroutines are verified, the program can be successfully opened, and if any intermediate link fails to pass the verification before starting the program, then the safety protection system will all recognize it as a failure and return to the prohibition of loading the program again. It can be seen that the authentication of login authority plays a vital role in the security protection of the entire computer system, and the security protection level and overall operation efficiency are relatively high.

IndexTerms **- Mining, databases, information, dataset, predictions, performance**

I. INTRODUCTION

The main process includes inputting the dongle after the computer is running and then verifying the media. If the conditions are met, the media will be further loaded, and if the media verification is not passed, the program will be forbidden. At this time, the entire system cannot continue to run, and the judgment efficiency is high. After the loading medium is passed, the next step is to verify the certificate file and then verify the user' name and password. After these subroutines are verified, the program can be successfully opened, and if any intermediate link fails to pass the verification before starting the program, then the safety protection system will all recognize it as a failure and return to the prohibition of loading the program again. It can be seen that the authentication of login authority plays a vital role in the security protection of the entire computer system, and the security protection level and overall operation efficiency are relatively high.

II. OBJECTIVES

- To share data securely and efficiently between many participants in cloud environment, with help of key generation. To achieve the same key agreement protocols is used along with the encryption and decryption technique. Same key is shared with the participants and to avoid malicious attack the fault tolerance property is used to deliver secure data.
- To provide security to all these components and interaction of these components with each other needs to be addressed.
- To improve the quality of service delivered on the network is another concern.
- To control loss over physical, Logical of system, and alternative control to client's assets, mismanagement of assets Are some additional concerns.

III. LITERATURE REVIEW

Jian Shen et al. proposed an efficient and secure block design-based key agreement protocol by extending the structure of the SBIBD to support multiple participants, which enables multiple data owners to freely share the outsourced data with high security and efficiency. Note that the SBIBD is constructed as the group data sharing model to support group data sharing in cloud computing. Moreover, the protocol can provide authentication services and a fault tolerance property. [1]

Mehdi Bahrami et al. proposed fields to establish a virtual IT department via the Internet. The cloud computing offers different virtual services like traditional IT department, such as storage, stream server and database server. The cloud provides a cost effective model through pay-per-use that allows each individual or businesses in healthcare start a cloud based service with minimum investment.[2]

Tessema Mengistu at al. proposed that The current Cloud Computing services are based on the "data center" approach, where hundreds of thousands of dedicated servers are setup to give the services. Setting up the data center for cloud is expensive and running the infrastructure needs expertise as well as a lot of resources such as high power for cooling, redundant power for

assured availability, etc. For example, 45% of the data center cost goes to the acquisition of servers, 25% goes to specialized infrastructure for fault tolerance, redundant power, cooling systems, and backup batteries, while electrical cost consumed by the machines accounts for 15% of the amortized total cost. In addition to the vast number of servers used in data centers, there are billions of Personal Computers (PCs) owned by individuals and organizations worldwide. [3]

Zhao Tianhai et al. proposed that Cloud computing is the new research and cooperation pattern for science computing. Keahey, et al. proposed one of the first cloud-based infrastructures for computational science, Science Cloud [1]. Software-as-a-service [2] is at the top end of the cloud computing stack, which is seen as a replacement to traditional software. With SAAS, the cloud operator provides end users with an integrated service which comprising hardware, software and development platform. The resource management is the key of application software service in science cloud computing. The optimization decomposition approach to solve cloud resource allocation for satisfying the cloud user's needs and the profits of the cloud providers [3].A new resource management framework presented provides efficient green enhancements within a scalable cloud computing architecture [4].

Wang Xiaoyu et al. proposed that Cloud computing has many definitions, but they are all pretty much the same. So called cloud computing, is composed of distributed processing, parallel processing and grid computing, development of a dynamic, good extension, virtualization technology is used to establish a unified infrastructure, services, applications and information resources pool, with distributed technology to the resource pool of infrastructure to effectively organize and run a computing model. Cloud computing as a new IT resources service mode, is composed of a large number of computer resources Shared IT resources pool, users have to use the data will be uploaded to the data resources pool, we can see IT as a huge data centres, again after the data integration to provide users with computing and storage services, to a great extent, improve the efficiency of resource use. After the cloud users upload their data to the cloud, the management of the data will no longer be controlled by the cloud users. At this time, the user data is in an uncontrollable domain, which makes the users lack sufficient trust in the cloud service provider, and of course, they do not want their data to be seen by others. [5]

Yanhong Shang1 et al.states that the outbreak of various information data leakage incidents have made computer network users increasingly demanding personal information security. The construction of a computer network information security environment can not only effectively ensure information security but also achieve greater effective protection of information security. This requires that the traditional information security protection measures be used as the basis to continuously increase the construction of information security. [6]

IV. MULTIDIMENSIONAL DATA SECURITY PROTECTION SYSTEM

4.1 Cloud Computing Services

Cloud services are infrastructure, platforms, or software that are hosted by third-party providers and made available to users through the internet. Cloud services facilitate the flow of user data from front-end clients (e.g., users' servers, tablets, desktops, laptops—anything on the users' ends), through the internet, to the provider's systems, and back. Cloud services promote the building of cloud-native applications and the flexibility of working in the cloud. Users can access cloud services with nothing more than a computer, operating system, and internet connectivity. Cloud computing has risen massively in terms of popularity in recent times. This is due to the way it reduces on-premise infrastructure cost and improves efficiency. Primarily, the cloud model has been divided into three major service categories:

Platform as a Service (PaaS)

Platform as a service refers to the cloud computing platform as a service, which provides the application running environment for users to meet their needs for the development environment. PaaS can integrate various resources, calculate the resource requirements according to the business requirements of customers, invoke the corresponding hardware resources through the interface provided by IasS, monitor the utilization of resources, and provide services to SaaS through the relevant interface. When using the service, users only need to use the API provided by the platform to easily develop and deploy applications without the need for cloud infrastructure management and control.

Software as a Service (SaaS)

SaaS is a mode in which application software is uniformly installed on various cloud platforms and users order application software services through the Internet. Users can use the whole software or only some functions of a certain software. The cloud service provider is responsible for the hardware facilities, management and maintenance of the software, so that users can use the software conveniently and quickly at any time and place through the Internet. Under the SaaS service mode, customers only need to pay for the corresponding services, which greatly reduces the operating cost of the enterprise, which is also the most efficient operation mode of network applications.

Infrastructure as a Service (IaaS)

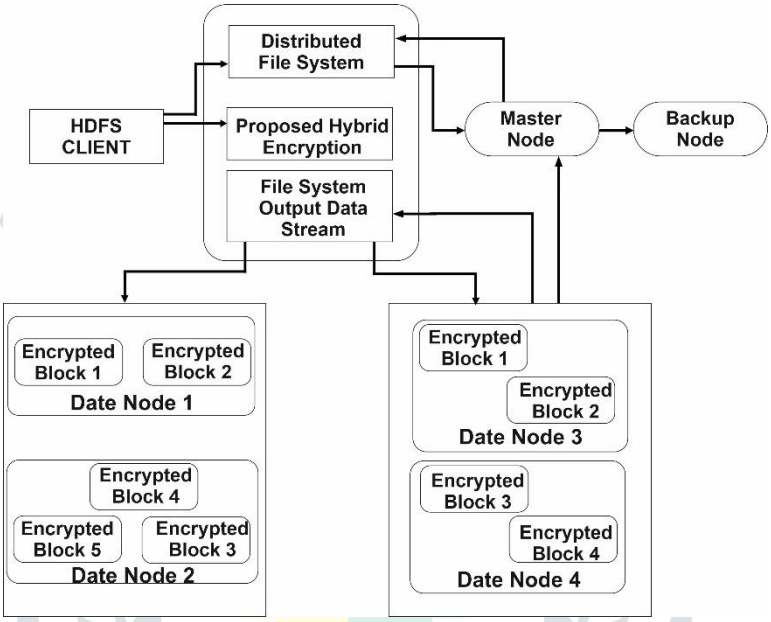
Infrastructure as a Service often provides the infrastructure such as servers, virtual machines, networks, operating system, storage, and much more on a pay-as-you-use basis. IaaS providers offer VM from small to extra-large machines. Infrastructure-as-a-Service, commonly referred to as simply "IaaS," is a form of cloud computing that delivers fundamental compute, network, and storage resources to consumers on-demand, over the internet, and on a pay-as-you-go basis. IaaS enables end users to scale and shrink resources on an as-needed basis, reducing the need for high, up-front capital expenditures or unnecessary "owned" infrastructure, especially in the case of "spiky" workloads.

B. Hash Tree Technology and HDFS Encryption Algorithm

The system gives a binary hash tree (tiger hash tree commonly used two binary hash tree, but also the form). It is often used in some distributed hash tree in distributed storage system or the anti-entropy mechanism (Antientropy), also called to entropy[11-13]. These applications include Amazon Dynamo and Apache Cassandra database, through to the entropy can do each synchronization of different nodes, each node keeps abreast of the latest information is. The characteristics of the hash tree is very clear: the leaf node is stored in the data file, and the nonleaf node is stored in the hash value of its child nodes (called Message Digest) of the non-leaf nodes of the Hash is called the path hash value, Hash value of leaf nodes is the real data.

V. DATAFIELD

Through block design-based key agreement protocol that supports multiple participants, which could flexibly extend the quantity of participants in associate extremely cloud setting in step with the structure of the block vogue. Supported the projected cluster info sharing model, we've got an inclination to gift general formulas for generating the common conference key K for multiple participants. Note that by creating the foremost of the (v; k + 1; 1)-block vogue, the procedure quality of the projected protocol linearly can increase with the quantity of participants and thus the communication quality is greatly reduced. In addition, the fault tolerance property of our protocol permits the cluster info sharing in cloud computing to set about to all totally different key attacks. A key agreement protocol is used to return up with a customary conference key for multiple participants to create positive the security of their later communications, and this protocol is applied in cloud computing to support secure and economical info sharing.



Fig, 5.1 Architecture of HDFS with algorithm process

VI. CONCLUSION

The proposed enables multiple participants to freely share the group data, which improves the efficiency of work in cooperative environments and has widespread potential applications. It also tries to ensure the security of data sharing within a group and how to efficiently share the outsourced data in a group manner are formidable challenges. Note that key agreement protocols have played a very important role in secure and efficient group data sharing in cloud computing. The main advantage of the symmetric balanced incomplete block design (SBIBD), by presenting a novel block design-based key agreement protocol that supports multiple participants, which can flexibly extend the number of participants in a cloud environment according to the structure of the block design was apparently design and help to provide security more than the previous system. The proposed group data sharing model, we present general formulas for generating the common conference key K for multiple participants. And the protocol linearly increases with the number of participants and the communication complexity is greatly reduced. In addition, the fault tolerance property of our protocol enables the group data sharing in cloud computing to withstand different key attacks.

VII. FUTURE WORK

Aiming at the security problems of the internal personnel of cloud service providers that are easy to be ignored, this paper puts forward the identity authentication and role-based access control strategies based on account and certificate, analyzes and studies the cloud security standards and legal maintenance, and puts forward the cloud security assessment system and relevant legal suggestions and measures to provide a strong guarantee for data security protection

VIII. ACKNOWLEDGMENT

We are thankful for the institutions for allowing us to submit a paper and interested to contribute and to evaluate the security in cloud computing through group data sharing agreement

REFERENCES

[1] G Abaya, S. A., & Gerardo, B. D. (2013, September). An education Jian Shen, Member, IEEE, Tianqi Zhou, Debiao He, Yuexin Zhang, Xingming Sun, Senior Member, IEEE, and Yang Xiang, Senior Member, IEEE, "Block Design-based Key Agreement for Group Data Sharing in Cloud Computing", 1545-5971 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information

[2] Mehdi Bahrami 1 and Mukesh Singhal 2, "A Dynamic Cloud Computing Platform for eHealth Systems", 2015 IEEE 17th International Conference on e-Health Networking, Applications and Services (Healthcom)

[3] Tessema Mengistu∗, Abdulrahman Alahmadi∗, Abdullah Albuali, Yousef Alsenani, and Dunren Che, "A "No Data Center" Solution to Cloud Computing", 2017 IEEE 10th International Conference on Cloud Computing

[4] Zhao Tianhai," The Key of Application Software Service in Science Cloud Computing", 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics

[5] Wang Xiaoyu, Gao Zhengming , "Research and Development of Data Security Multidimensional Protection System in Cloud Computing Environment" , 2020 International Conference on Advance in Ambient Computing and Intelligence (ICAACI)

[6] Yanhong Shang1 and Jing Zhang," Computer Multimedia Security Protection System Based on the Network Security Active Defense Model", Hindawi, Advances in Multimedia, Volume 2021, Article ID 8792105, 9 pages, https://doi.org/10.1155/2021/8792105

[7] L. Zhou, V. Varadharajan, and M. Hitchens, "Cryptographic rolebased access control for secure cloud data storage systems," Information Forensics and Security IEEE Transactions on, vol. 10, no. 11, pp. 2381–2395, 2015.

[8] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, "Secure cloud storage meets with secure network coding," in IEEE INFOCOM, 2014, pp. 673–681.

[9] 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.

[10] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[11] J. Shen, H. Tan, S. Moh, I. Chung, and J. Wang, "An efficient rfid authentication protocol providing strong privacy and security," Journal of Internet Technology, vol. 17, no. 3, p. 2, 2016.

[12] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, "An efficient protocol for authenticated key agreement," Designs Codes and Cryptography, vol. 28, no. 2, pp. 119–134, 2010.

[13] X. Yi, "Identity-based fault-tolerant conference key agreement," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, pp. 170–178, 2004.

[14] R. Barua, R. Dutta, and P. Sarkar, "Extending joux's protocol to multi party key agreement (extended abstract)." Lecture Notes in Computer Science, vol. 2003, pp. 205–217, 2003.

[15] J. Shen, S. Moh, and I. Chung, "Identity-based key agreement protocol employing a symmetric balanced incomplete block design," Journal of Communications and Networks, vol. 14, no. 6, pp. 682–691, 2012.

[16] B. Dan and M. Franklin, "Identity-based encryption from the weil pairing," Siam Journal on Computing, vol. 32, no. 3, pp. 213–229, 2003.

[17] S. Blakewilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in IMA International Conference on Cryptography and Coding, 1997, pp. 30–45.

[18] I. Chung and Y. Bae, "The design of an efficient load balancing algorithm employing block design," Journal of Applied Mathematics and Computing, vol. 14, no. 1, pp. 343–351, 2004.

[19] O. Lee, S. Yoo, B. Park, and I. Chung, "The design and analysis of an efficient load balancing algorithm employing the symmetric balanced incomplete block design." Information Sciences, vol. 176, no. 15, pp. 2148–2160, 2006.

[20] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, pp. 79–88, 2011.

[21] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.

[22] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1–1, 2015.

[23] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1–1, 2016.

[24] S. D. C. D. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Encryption policies for regulating access to outsourced data," Acm Transactions on Database Systems, vol. 35, no. 2, pp. 78–78, 2010.

[25] H. Guo, Z. Li, Y. Mu, and X. Zhang, "Cryptanalysis of simple three-party key exchange protocol," Computers and Security, vol. 27, no. 1-2, pp. 16–21, 2008.

[26] Z. Tan, "An enhanced three-party authentication key exchange protocol for mobile commerce environments," Journal of Communications, vol. 5, no. 5, pp. 436–443, 2010.

[27] Y. M. Tseng, "An efficient two-party identity-based key exchange protocol." Informatica, vol. 18, no. 1, pp. 125–136, 2007.

[28] A. Shamir, "Identity-based cryptosystems and signature schemes," Lecture Notes in Computer Science, vol. 21, no. 2, pp. 47–53, 1985.

[29] E. Bresson, O. Chevassut, D. Pointcheval, and J. J. Quisquater, "Provably authenticated group diffie-hellman key exchange," Acm Transactions on Information and System Security, vol. 10, no. 3, pp. 89–92, 2001.