INFORMATION EXCHANGE FRAMEWORK TOENHANCE CLOUD STORAGE SAFETY IN THEPERIOD OF MASSIVE DATA

Dr. Thanveer Jahan, Associate ProfessorHead of the DepartmentCSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban

J.Madhavi Assistant Professor CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S)

S.Soumya Rao (20641A66E3), UG student CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S)

T. Sri Varsh (20641A66D4), UG student CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S)

B.Charan (21645A6602), UG student CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S)

G. Kiran Kumar (21645A6610), UG student CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S)

ABSTRACT

The Title refers to "A Framework for information exchange to improve the cloud storage safety in the era of massive data.Cloud computing is a new computing model, in which all resource on Internet form a cloud resource pool and can be allocated to different applications and services dynamically.In contrast to traditional solutions, cloud provider stores the shared data in the large data centers outside the trust domain of the data owner, which may trigger the problem of data confidentiality. This paper proposes a secret sharing group key management protocol (SSGK) to protect the communication process and shared data from unauthorized access. Different from the prior works, a group key is used to encrypt the shared data and a secret sharing scheme is used to distribute the group key in SSGK. The extensive security and performance analyses indicate that our protocol highly minimizes the security and privacy risks of sharing data in cloud storage and saves about 12% of storage space

INTRODUCTION

The emerging technologies about big data such as Cloud Computing, Business Intelligence, Data Mining , Industrial Information Integration Engineering(IIIE) and Internet-of-Things have opened a new era for future Enterprise Systems(ES) . Cloud computing is a new computing model, in which all resource on Internet form a cloud resource pool and can be allocated to different applications and services dynamically. Compared with traditional distribute system, a considerable amount of investment saved and it brings exceptional elasticity, scalability and efficiency for task execution. By utilizing Cloud Computing services, the numerous enterprise investments in building and maintaining a supercomputing or grid computing environment for smart applications can be effectively reduced. Despite these advantages, security requirements dramatically rise when storing personal identifiable on cloud environment. This raise regulatory compliance issues since migrate the sensitive data from federate domain to distribute domain. To take the benefit enabled by big data technologies, security and privacy issues, must be addressed firstly. Building security mechanism for cloud storage is not an easy task. Because shared data on the cloud is outside the control domain of legitimate participants, making the shared data usable upon the demand of the legitimate users should be solved. Additionally, increasingnumber of parties, devices and applications involved in the cloud leads to the explosive growth of numbers of access points, which makes it more difficult to take proper access control. Lastly, shared data on the cloud are vulnerable to lost or incorrectly modified by the cloud provider or network attackers. Protecting shared data from unauthorized deletion, modification and fabrication is a difficult task. Conventionally, there are two separate methods to promote the security of sharing system. One is access control, in which only authorized

user recorded in the access control table has the access privilege of the shared data. The other method is group key management in which a group key is used to protect the shared data. Although access control makes the data only be accessed by legitimate participants, it cannot protect the attack from cloud providers. In the existing group key sharing systems, the group key is generally managed by an independent third party. Such methods assume that the third party is always honest. However, the assumption is not always real especially in the environment of cloud storage. To address the security problem of sharing data on the cloud storage, a secret sharing group key managementprotocol is proposed in the paper and the following means are taken by our protocol to help detect or prevent frauds. Firstly, in order to make the shared data usable upon demand by the legitimate users, symmetric encryption algorithms are used to encrypt the shared data. Once one data owner wants to share data with others, the decryption key is distributed to the legitimate sharers by the data owner. Secondly, the key used to decrypt the shared data controls the access permission for shared data. Asymmetric encryption algorithms are used to encrypt the interactive message and makes only legitimate participants have the ability to decrypt the key. Thirdly, in case of shared data being known by unauthorized users, this protocol uses secret sharing scheme to assign key to the legitimate participants. By adding security mechanism to conventional servic oriented clouds, we obtain a security aware cloud and guarantee the privacy of data sharing on cloud storage. Building security mechanism on cloud storage may accelerate the deployment of a cloud inmission

LITERATURE SURVEY
TITLE:-Authentication by Email Reception
AUTHORS:-Don Libes
ABSTRACT:-This paper describes the use of email addresses as an authentication mechanism forpublic access servers. Intended for untrusted and low-risk environments, this mechanism provides reasonable security at very low cost to both user and server administrator. In particular, the initialand subsequent registrations are totally automated, and problem detection/resolution is highly automated. Keywords: security, authentication, email reception, email address Introduction In this paper, I describe the use of email reception as an authentication mechanism for public access servers, such as email- and Web-based servers in untrusted and low-risk environments [DoD]. Even the simplest implementation provides security that is significantly better than trust and requires significant power to crack. Despite its security limitations, this type of authentication should be attractive for a large percentage of servers that are now currently trust-based. In particular, thesystem administration cost...

TITLE:-On minimizing energy cost in Internet-scale systems with dynamic data
AUTHORSP. Zhao, W. Yu, S. Yang, X. Yang, and J. Lin
ABSTRACT:-With the tremendous growth of cloud computing and Internet-scale online services, massive geographically distributed infrastructures have been deployed to meet the increasing demand, resulting in significant monetary expenditure and environmental pollution caused by energy consumption. In this paper, we investigate how to minimize the long-term energy cost of dynamic Internet-scale systems by fully exploiting the energy efficiency in geographic diversity and variation over time. To this end, we formulate a stochastic optimization problem by considering the fundamental uncertainties of Internet-scale systems, such as the dynamic data. We develop a dynamic request mapping algorithm to solve the formulated problem, which balances the tradeoff between energy cost and delay performance. Our designed algorithm
makes real-time decisions based on current queue backlogs and system states, and does not require any knowledge of stochastic job arrivals and service rates caused by dynamic data queries. We formally prove the optimality of our approach. Extensive trace-driven simulations verify our theoretical analysis and demonstrate that our algorithm outperforms the baseline strategies with respect to system cost, queue backlogs, and delay.

TITLE:-Risk and safety program performance evaluation and business process modeling
AUTHORS:-K.-Y. Teng, S. A. Thekdi, and J. H. Lambert

ABSTRACT:-There is increasing need for agencies to coordinate their interdependent risk assessment, risk management, and risk communication activities in compliance with risk program guidelines. In particular, there is a challenge to measure risk program compliance and maturity to guidelines such as the U.S. Office of Management and Budget (OMB) memorandum "Updated Principles for Risk Analysis" among others. This paper demonstrates a systemic approach to evaluate large-scale risk program maturity with utilization of business process modeling and self- assessment methods. This approach will be helpful to agencies implementing risk guidelines such as those of the OMB, the U.S. Government Accountability Office, the U.S. Department of Homeland Security, the U.S. Department of Defense, and others. This paper will be of interest to risk managers, agencies, and risk and safety analysts engaged in the conception, implementation, and evaluation of risk and safety programs.

TITLE:-A fuzzy preference tree-based recommender system for personalized business-to- business E-services
AUTHORS:-D.Wu, G. Zhang, and J. Lu

ABSTRACT:-The Web creates excellent opportunities for businesses to provide personalized online services to their customers. Recommender systems aim to automatically generate personalizedsuggestions of products/services to customers (businesses or individuals). Although recommender systems have been well studied, there are still two challenges in the development of a recommender system, particularly in real-world B2B e-services: (1) items or user profiles often present complicated tree structures in business applications, which cannot be handled by normal item similarity measures and (2) online users' preferences are often vague and fuzzy, and cannot be dealt with by existing recommendation methods. To handle both these challenges, this study first proposes a method for modeling fuzzy tree-structured user preferences, in which fuzzy set techniques are used to express user preferences. A recommendation approach to recommending tree-structured items is then developed. The key technique in this study is a comprehensive tree matching method, which can match two tree- structured data and identify their corresponding parts by considering all the information on tree structures, node attributes, and weights. Importantly, the proposed fuzzy preference tree-based recommendation approach is tested and validated using an Australian business dataset and the MovieLens dataset. Experimental results show that the proposed fuzzy tree-structured user preference profile reflects user preferences effectively and the recommendation approach demonstrates excellent performance for tree-structured items, especially in e-business appli cation.

PROBLEM STATEMENT
The traditional solution cloud provider stores shared data in large data centers outside the domain of the data owner.This leads to data confidentiality.
LIMITATION OF SYSTEM
Massive Data cannot work effectively in traditional method.The attribute-based techniques are failed to protect user attribute..

PROPOSED SYSTEM
The main contributions are as follows:
Toaddressthesecurityproblemofsharingdataoncloudstorage.once one data owner wants to share data with others; decryption key is generated by data owner.Secret sharing key management protocol (SSGK) helps to detect or prevent frauds.
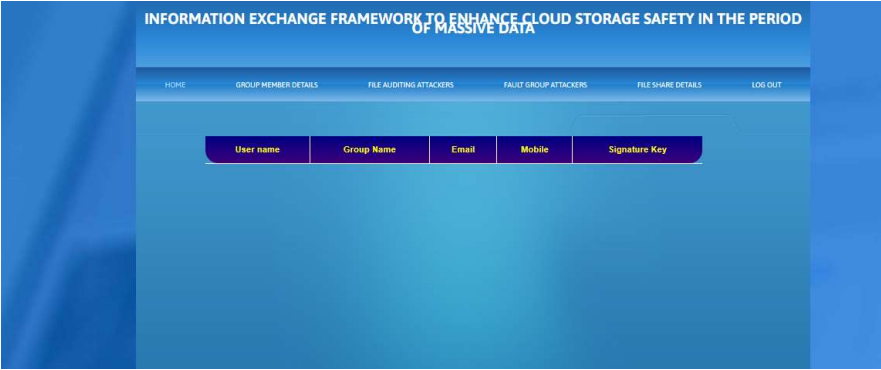
4.1 ADVANTAGES:

Symmetric & Asymmetric encryption algorithms used.If shared data is known by un authorized users. This protocol uses secret sharing scheme to assign key to legitimate user.
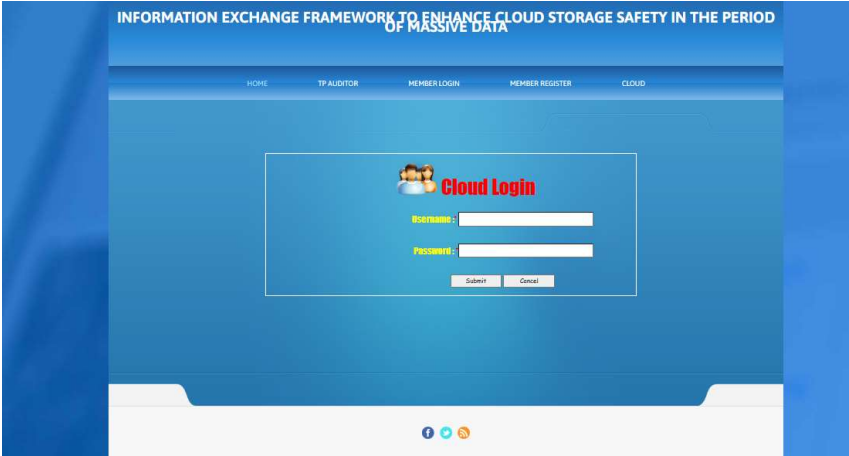
SYSTEM ARCHITECTURE
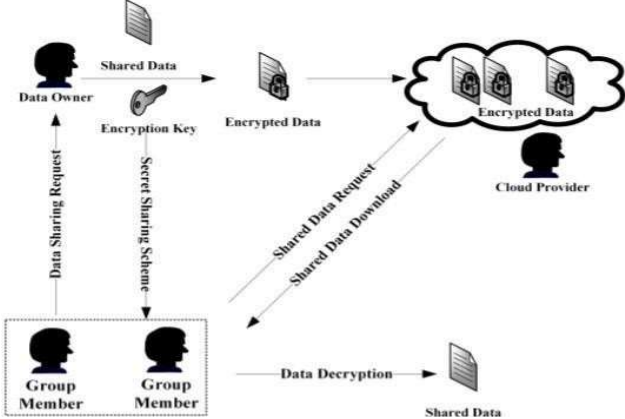
EXPECTED RESULTS

GROUP MEMBERS DETAILS

CLOUD LOGIN

TP AUDITOR

Member registration page

Home page

CONCLUSION

In this paper, we propose a novel group key management protocol for the data sharing in the cloud storage. .In SSGK, we uses RSA and verifed secret sharing to make the data owner achieve _ne-grained control over the out sourced data without relying on any third party. In addition, we give detailed analysis of possible attacks and corresponding defenses, which demonstrates that GKMP is secure under weaker assumptions. Moreover we demonstrate that our protocol exhibits less storage and computing complexity .Security mechanism in our scheme guarantees the privacy of grids data in cloud storage. Encryption secures the transmission on the public channel; verified security scheme make the grids data only accessed by authorized parties. The better performance in terms of storage and computation make our scheme more practical. The problem of forward and backward security in group key management may require some additions to our protocol .An efficient dynamic mechanism of group members remains as future work.

FUTURESCOPE

The future scope for information exchange frameworks to enhance cloud storage safety in the period of massive data projects is very promising. As the volume of data stored in the cloud continues to grow, so too does the need for secure and efficient ways to exchange information.One way to improve the safety of cloud storage is to use encryption to protect data at rest and in transit. However, encryption can also make it difficult to exchange data securely. One way to address this challenge is to use a key management system (KMS) to manage encryption keys. A KMS provides a secure way to store and distribute encryption keys, and it can also be used to automate the encryption and decryption process.Another way to improve the safety of cloud storage is to use a data loss prevention (DLP) solution. A DLP solution can help to identify and protect sensitive data stored in the cloud. For example, a DLP solution can be used to prevent users from uploading sensitive data to the cloud, or from sharing sensitive data with unauthorized users.In addition to encryption and DLP, there are a number of other information exchange frameworks that can be used to enhance cloud storage safety. For example, organizations can use identity and access management (IAM) solutions to control who has access to their cloud data. Organizations can also use auditing and logging solutions to track who is accessing their cloud data and what they are doing with it.

In the period of massive data projects, it is especially important to use information exchange frameworks to enhance cloud storage safety. This is because massive data projects often involve the storage and processing of sensitive data. By using information exchange frameworks, organizations can help to protect their data from unauthorized access, theft, and loss.Here are some specific examples of how information exchange frameworks can be used to enhance cloud storage safety in the period of massive data projects:Use a KMS to manage encryption keys. This will allow organizations to securely exchange data with other organizations, even if they are using different cloud providers.Use a DLP solution to protect sensitive data. This will help to prevent sensitive data from being uploaded to the cloud or shared with unauthorized users.Use an IAM solution to control access to cloud data. This will ensure that only authorized users have access to cloud data.Use an auditing and logging solution to track access to cloud data. This will help organizations to identify and respond to security incidents.In addition to these specific examples, information exchange frameworks can be used to enhance cloud storage safety in a number of other ways. For example, organizations can use information exchange frameworks to:Share threat intelligence. Organizations can use information exchange frameworks to share information about security threats with other organizations. This can help organizations to protect themselves from known threats.Collaborate on security research. Organizations can use information exchange frameworks to collaborate on security research. This can help organizations to identify and address new security threats.Develop industry standards. Organizations can use information exchange frameworks to develop industry standards for cloud security. This can help to improve the overall security of cloud

storage.Overall, the future scope for information exchange frameworks to enhance cloud storage safety is very promising. By using information exchange frameworks, organizations can help to protect their data from unauthorized access, theft, and loss. This is especially important in the period of massive data projects, when organizations are often storing and processing sensitive data.

REFERENCES

[1]   P. Zhao, W. Yu, S. Yang, X. Yang, and J. Lin, ``On minimizing energy cost in Internet-scale systems with dynamic data," IEEE Access, vol. 5,pp. 20068_20082, 2017.

[2]   D.Wu, G. Zhang, and J. Lu, ``A fuzzy preference tree-based recommender system for personalized business-to-business E-services," IEEE Trans.Fuzzy Syst., vol. 23, no. 1, pp. 29_43, Feb. 2015.

[3]   X. Wu, X. Zhu, G.-Q. Wu, and W. Ding, ``Data mining with big data,"IEEE Trans. Knowl. Data Eng., vol. 26, no. 1, pp. 97_107, Jan. 2014.

[4]   X. Shi, L. X. Li, L. Yang, Z. Li, and J. Y. Choi, ``Information flow in reverse logistics: An industrial information integration study," Inf. Technol.Manage., vol. 13, no. 4, pp. 217_232, Dec. 2012.

[5]   N. Bizanis and F. A. Kuipers, ``SDN and virtualization solutions forthe Internet of Things: A survey," IEEE Access, vol. 4, pp. 5591_5606, May 2016.

[6]   S. Li, L. Xu, X. Wang, and J. Wang, ``Integration of hybrid wireless networks in cloud services oriented enterprise information systems," Enterprise Inf. Syst., vol. 6, no. 2, pp. 165_187, Nov. 2012.

[7]   K.-Y. Teng, S. A. Thekdi, and J. H. Lambert, ``Risk and safety program performance evaluation and business process modeling," IEEE Trans.Syst., Man, Cybern. A, Syst. Humans, vol. 42, no. 6, pp. 1504_1513, Nov. 2012.

[8]   Z. Fu, X. Sun, S. Ji, and G. Xie, ``Towards efficient content-aware search over encrypted outsourced data in cloud," in Proc. 35th Annu. IEEE Int.Conf. Comput. Commun. (INFOCOM), Apr. 2016, pp. 1_9.

[9]   J. Han, W. Susio, Y. Mu, and J. Hou, ``Improving privacy and security indecentralized ciphertext-policy attribute-based encryption," IEEE Trans.Inf. Forensics Security, vol. 10, no. 3, pp. 665_678, Mar. 2015.

[10] D. Zou, Y. Xiang, and G. Min, ``Privacy preserving in cloud computingenvironment," Secur. Commun. Netw., vol. 9, no. 15, pp. 2752_2753Oct. 2016.