Group Data Sharing using Cloud Computing

Rashmi Raj[1], Gitanjali Mahanwar[2], Pooja Devadiga[3], Snehal Bhoge[4], Manjusha Tatiya[5]

Student[1234], Assistant Professor[5]
Department Of Computer Engineering,
Indira College of Engineering and Management, Pune, India

Abstract : Cloud computing is said to be the service oriented computing technology, which are affordable and flexible over the internet. In past few years the cloud has become more matured and provided many services, one of the primary service is data sharing in Group, where the data can be easily shared from one member to another. However, while sharing the data security is one of the primary concern. In past several methodology has been proposed. However, these methods lacked from the feasibility. Hence, in this paper we have propose methodology is based on the selection scheme. Here General Group Key is generated and moreover General Key agreement protocol is decentralized based model where the data are controlled by the owner within the same group. Moreover, the proposed methodology is evaluated by analyzing the comparative analysis based on the various number of parameter. Result Analysis suggest that our methodology simply outperforms the existing one.

IndexTerms- Cloud Computing, security, Group data sharing.

I. INTRODUCTION

In recent decades as the concept of cloud computing rises, cloud storage is said to be the one of the hotspots of the storage of information. It basically refers to a model, which refers to the model that provides the data storage. Here, CSP (cloud service provider) is directly responsible for making data available as well as accessible according to the requirement of use. Storage capacity is either bought or leased from provider to store the data by the individual or organization. This service can easily be accessed through the API or the application, which utilizes the API such as cloud storage gateway.

Moreover, in the past few years, it has been observed that the demand of cloud storage has been phenomenal in accordance with the use of personal as well as business purpose, since it is highly based on the virtualized infrastructure and much more flexible in terms of multi-tenancy, scalability and availability. They are typically knows as object storage such as Microsoft azure, amazon s3 and oracle cloud storage [4]. Since the cloud, computing gives us the feature of pay as you go service, the organization wants to pay only for the service they use, and cloud service provides exactly the same. Business using the CS can actually reduce up to 70% of energy consumption. CSP is totally responsible for the maintenance of the data and as well as the other tasks such as buying the additional storage capacity. Since the backup of the data are located in several places in the globe, it can also be applicable as the proof backup of natural disaster. Meanwhile, cloud storage is one service, which is not referred to the physical device, but it is the aggregation of many server and storage for its users.

II. LITERATURE SURVEY

Data communication through a network is secured using an efficient technique i.e, Cryptography. Encryption and Decryption are the basic operations performed by efficient algorithms. Cryptography based on block ciphers use Key-dependent ciphers for encryption and decryption. The efficiency of these systems depends on the security and the speed of the algorithm. Advanced Encryption Standard (AES) is an efficient block cipher which comprises of AES-128, AES-192 and AES-256 block ciphers. The key size used in the cipher specifies the number of rounds repeated to convert the plain text into cipher text. To transform the cipher text into plain text, reverse rounds are applied using the same secret key. This research paper has proposed two methods to enhance the performance of conventional AES, using Genetic algorithm and Neural network. This will make the existing cryptosystem more complex and stronger against cryptanalytic attacks. But the complexity lies in choosing the fitness function of GA, number of adaptive iterations and the weight of the neuron in NN. The encryption process needs to be adaptive and dynamic in order to face any cryptanalytic attacks. Increasing the complexity of the algorithm is one way to prevent the attacks. The introduced complexity increases the execution time of the algorithm which leads to timing attacks. The attempts to propose two enhanced AES cryptosystem by employing Genetic algorithm (GA) in SPboxes and modification of AES by implementing nonlinear neural network (NN) in SP network to increase the security against timing attack and reduce the computational time of the proposed system. Both GA and NN are used in key. This motivates for encryption but it is complex to use and it needs to decrypt the plain text[2].

The connection-level stability of a network employing congestion control. In particular, studied how the stability region of the network (i.e., the set of offered loads for which the number of active users in the network remains finite) is affected by congestion control. This time-scale separation assumption is removed and it is shown that the largest possible stability region can still be achieved by a large class of control algorithms. A second assumption often made in prior work is that the packets of a source (or user) are offered to each link along its path instantaneously, rather than passing through one queue at a time. They show that connection-level stability is again maintained when this assumption is removed, provided that a back-pressure scheduling algorithm is used jointly with the appropriate congestion controller. CONGESTION control is a key functionality in modern communication networks. The objective of congestion control is to regulate the data rate at which each user injects data into the network such that: 1) the network capacity is fully utilized, 2) excessive congestion inside the network is avoided, and 3) some form of fairness (in terms of the amount of service that each user receives) is ensured. These objectives can be mapped to a global optimization problem that maximizes the total system utility, where different fairness objectives can be achieved by appropriately choosing the utility functions. [3]

The problem of secure and fault-tolerant communication in the presence of adversaries across a multihop wireless network with frequently changing topology. To effectively cope with arbitrary malicious disruption of data transmissions, the system propose and evaluate the secure message transmission (SMT) protocol and its alternative, the secure single-path (SSP) protocol. Among the salient features of SMT and SSP is their ability to operate solely in an end-to-end manner and without restrictive assumptions on the network trust and security associations. As a result, the protocols are applicable to a wide range of network architectures. It demonstrate that highly reliable communication can be sustained with small delay and small delay variability, even when a substantial portion of the network nodes systematically or intermittently disrupt communication. SMT and SSP robustly detect transmission failures and continuously configure their operation to avoid and tolerate data loss, and to ensure the availability of communication. This is achieved at the expense of moderate transmission and routing overhead, which can be traded off for delay. Overall, the ability of the protocols to mitigate both malicious and benign faults allows fast and reliability .[4]

The consideration of a wireless network where interference is treated as noise, and studied the nonconvex problem of sum rate maximization by power control. This focus on finding approximately optimal solutions that can be efficiently computed to this NP-hard problem by studying the solutions to two related problems, the sum rate maximization using a signal-to-interference-plus-noise ratio ( ) approximation and the max-min weighted optimization. These two problems have also been studied before, but now there is a faster algorithms, often independent of parameter tuning and network configuration. This shows that these two problems are intimately connected, can be solved efficiently by algorithms with fast convergence and minimal parameter configuration, and can yield high-quality approximately optimal solutions to sum rate maximization in the low interference regime. As an application of these results, the analysis of the connection-level stability of cross-layer utility maximization in the wireless network, where users arrive and depart randomly and are subject to congestion control, and the queue service rates at all the links are determined by the sum rate maximization problem. In particular, determines the stability region when all the links solve the max-min weighted problem, using instantaneous queue sizes as weights. An important and challenging direction for future work is to characterize a lower bound on the achievable fraction of the stability region that is independent of the problem instance parameters.[5]

The demonstratation for the first time WDM-PON secure optical communication based on chaotic-laser, and real-time online fiber-fault detection and location simultaneously, which will significantly improve WDM-PON reliability and reduce the cost of operation and maintenance. The increasing evidence indicates that the survivability of the future network relies more and more on the security of information transportation. Because of the broadband, perfect security, simple realization at the physical layer and the good real-time properties, the chaotic-light secure communication is attracting more and more attention, and lots of simulation and experimental results are reported in the aspect of long-distance transmission and wavelength division multiplexing, etc. Much attention is also paid to the chaotic-light secure communication applied to the passive optical network (PON), and a simulation result has been reported . Since the structure and overall arrangement of optical access networks is complex and meanwhile, the amount of operational fiber is huge, failures of optical fiber links occur more frequently, and therefore, the cost and operation, administration and maintenance (OAM) stays at a high level. The real-time online fiber-fault detection and location in the optical access network with traditional optical domain reflector (OTDR) is complex and costly, and has low resolution of the fault location. The proposed method saves a number of expensive devices or complex equipments, such as the light source in the traditional OTDR, and it has merits of being realized simply and low cost. Thus, the OAM is significantly reduced, and it will be widely employed.[6]

III. CONCLUSION

Group data sharing in the cloud plays an eminent role when the data has to be distributed among the others. Moreover, security is one of the big concern when it comes to preserving the privacy. In this research work, we have developed a methodology based on the selection scheme, which helps in securing the data. We are providing cloud base encryption system for database for security purpose. Data is encrypted during the transaction which never decrypt .

REFERENCES

[1] "Efficient and Secure Group Data Sharing Model based on Selection scheme in Cloud environment." IEEE paper Author Shubhangi Patil & Rekha Patil.
[2]"Enhanced AES Cryptosystem by using Genetic Algorithm and Neural Network in S-box" By K . Kalaiselvi Dr. Anand Kumar
[3] "On the Connection-Level Stability of Congestion-Controlled Communication Networks" Xiaojun Lin, Member, IEEE, Ness B. Shroff, Fellow, IEEE, and R. Srikant, Fellow, IEEE
[4] "Secure Data Communication in Mobile Ad Hoc Networks" Panagiotis Papadimitratos, Member, IEEE, and Zygmunt J. Haas, Senior Member, IEEE
[5] "Fast Algorithms and Performance Bounds for Sum Rate Maximization in Wireless Networks" Chee Wei Tan, Senior Member, IEEE, Mung Chiang, Fellow, IEEE, and R. Srikant, Fellow, IEEE
[6] "Demonstration of Chaotic-Laser Based WDM-PON Secure Optical Communication and Real-time Online Fiber-Fault Detection and Location" Xinyu Dou1 , Hongxi Yin1,*, Yang Hao2 , Hehe Yue1 , Xiaoyong Qi2 , Yu Jin1 , Jie Qin1 , Lin Li2 1 Lab of Optical Communications and Photonic Technology, School of Information and Communication Engineering, Dalian University of Technology, Dalian, China 2 HAEPC Information & Telecommunication Company, Zhengzhou, China
[7] "NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users" Anmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang.
[8]"Enabling Efficient and Protected Sharing of Data in Cloud Computing" D.Aarthi.
[9]"Block Design-based Key Agreement for Group Data Sharing in Cloud Computing" Jian Shen, Member,Tianqi Zhou, Debiao He, Yuexin Zhang, Xingming Sun, and Yang Xiang.
[10]" Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud 2016" Dnyanada Dongare Asst Prof.Vijayalakshmi Kadroli.
[11]"Privacy-Preserving Cloud Auditing for Multiple Users Scheme With Authorization and Traceability" XIAODONG YANG , MEIDING WANG, TING LI, RUI LIU, AND CAIFEN WANG.