www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 108-110

e-ISSN : 2583-1062

Impact Factor : 5.725

DEVELOPING MULTIPARTY ACCESS CONTROL MECHANISM FOR MULTI-OWNER BY PROVIDING SECURED DATA GROUP SHARING USING CLOUD COMPUTING

J.Charlin Carmal[1], Dr.V.N.Raja Varman[2], Dr.S.Geetha[3]

[1]Final Year M.Tech CFIS, Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India.

[2]Professor, Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India.

[3]Head of Department, Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India.

ABSTRACT

Cloud services uses the cryptographic techniques that employs encryption techniques to secured that will be used or stored in the cloud and also provide the data confidentiality in cloud computing. Cloud computing uses the concept of cipher text, which encrypts the text based on an algorithm but it could not provide the privacy aspects over multiple owners. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Thus it makes co- owners unable to control data disseminators can actually disseminate their data. Because of the frequent change in membership, sharing data while providing privacy aspects is still a challenging issue. The data owners could broadcast encrypted data to a group of receivers at one time by specifying these receiver`s identities in a convenient and secure way. Thus we provide a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing environments Disseminate the data over the different user with satisfying constrain access policies with multi party access control mechanism in the cipher text. By using this functionality, we can restrict the users accessibility based on their rights and constrains over the data. Data co-owners can add new access policies for the privacy controls. It includes the full permit, owner priority and majority permit to solve the privacy conflicts problem caused by different access policies.

1. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, continuous, on-demand network access to a shared pool of configurable computing resources(e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. There are several different aspects of Cloud Computing that must be looked into. They are given below. Sharing computational resources, storage, services and applications with other tenants residing on same physical or logical platform at the provider’s place. Increase in the number of systems, bandwidth, and storage space. Users can increase or decrease their computing resources as needed. Users to pay for only the resources they actually use and for the time they require them. Self-provisioning of resources: users self-provision resources such as software, storage and network.

2. LITERATURE SURVEY

Nikos Bizanis et.al, in this article, we survey the state-of-the-art on the application of SDN and NV to IoT. We review some general SDN-NV-enabled IoT architectures, along with real-life deployments and use-cases.

Olivier Flauzac et.al, we first present a new SDN based architecture for networking with or without infrastructure, that we call an SDN domain.Next, we propose a second architecture to include sensor networks in an SDN-based network and in a domain.

3. EXISTING SYSTEM

In Existing System, Cloud services with cryptographic techniques cannot provide the privacy aspects for multiple owners and co-owners over their data stored in the cloud. It makes the owners unable to control the data disseminators can actually disseminate their data’s. Cloud computing uses the concept of cipher text, which encrypts the text based on an algorithm but it could not provide the privacy aspects over multiple owners. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Thus it makes co-owners unable to control data disseminators can actually disseminate their data. Because of the frequent change in membership, sharing data while providing privacy aspects is still a challenging issue. The data owners could broadcast encrypted data to a group of receivers at one time by specifying these receiver`s identities in a convenient and secure way.. It includes the full permit, owner priority and majority permit to solve the privacy conflicts problem caused by different access policies.

4. PROPOSED SYSTEM

We propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic groups. We provide a secure way for key distribution without any secure communication channels. Thus user can securely obtain their private keys from the group manager without any certificate authorities due to the verification for the public key of the user. We propose secure data sharing scheme which can be protected from collusion attack. The revoked user cannot be able to get the access over the revoked data of that user in the cloud group sharing. Our scheme achieves the secure user revocation with the help of dynamicfunctionality.

5. PURPOSE OF THE RESEARCH

We address the problem of IoT security. With the help of SDN, we aim to prevent the attacks at network level instead of device level. Our objective is to protect the IoT devices from malicious attacks and reduce the damage upon an attack. The attack may be launched from the IoT device itself or the device is the target. This helps in fast identification of attacks on IoT devices and initiation of mitigation procedure as appropriate. We have used machine learning techniques to detect anomalies in the traffic.

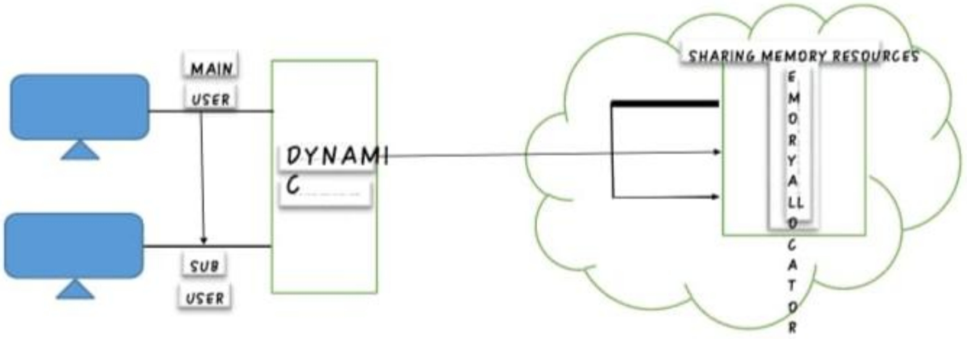

Figure 1. Architecture Diagram

5.1 List of Modules

- Secure Dynamic Auditing
- Algorithms and Constructions for DynamicAuditing
- DataUpdate
- Group Auditing for Multi-Owner and Multi-Cloud.

5.2 Modules Description

Secure Dynamic Auditing

In cloud storage systems, the data owners will dynamically update their data. As an auditing service, the auditing protocol should be designed to support the dynamic data, as well as the static archive data.

6. CONCLUSION AND FUTURE ENHANCEMENT

There are different analysis that are conducted to look into the security of multicloud and a classification about data at rest and data in transit is required for efficient handling of data security features. Each approach discusses briefly about the algorithm used and the architecture needed to enhance the security. A novelty in multi-cloud security should have the flavors of cryptographic functions combined with the selection of best algorithm for encryption of data together with Deduplication measures to ensure one copy of the data is stored thereby ensuring data Integrity and ensure availability**.**

7. REFERENCES

[1] ITU report, “The Internet of Things,” 2005.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Elsevier FGCS, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] Gartner report, “Forecast: IoT Security, Worldwide,” 2016.

[4] IDC report, “Internet of Things: Security Practices,” 2016.

[5] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “A multifaceted approach to understanding the botnet phenomenon,” 6th ACM SIGCOMM conference on Internet measurement, pp. 41–52, 2006.

[6] Dyn attack 2016, http://dyn.com/blog/dyn-analysis-summary-of-fridayoctober-21-attack/, [Online; accessed 18-07-2017].

[7] Mirai Malware 2016, http://blog.malwaremustdie.org/2016/08/mmd0056-2016-linuxmirai-just.html, [Online; accessed 18-07-2017].

[8] K. Palani, E. Holt, and S. Smith, “Invisible and forgotten: Zero-day blooms in the IoT,” IEEE PerCom Workshops, pp. 1–6, 2016.

[9] H. Zhang, A. C. Berg, M. Maire, and J. Malik, “SVM-KNN: Discriminative nearest neighbor classification for visual category recognition,” IEEE CVPR Conference, pp. 2126–2136, 2006.

[10] K. Sood, S. Yu, and Y. Xiang, “Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review,” IEEE Internet of Things Journal, vol. 3, no. 4, pp. 453–463, 2016.