Journal of Advances and Scholarly Researches in Allied Education
Vol. 18, Issue No. 4, July-2021, ISSN 2230-7540

A Study the Secure Data Sharing in Cloud Environment

Saket Nigam[1]*, Dr. Rajeev Yadav[2]

[1] Research Scholar, Shri Krishna University, Chhatarpur M.P.

[2] Professor, Shri Krishna University, Chhatarpur M.P.

Abstract - Cloud computing is a technology offering services in which resources are provisioned on an on-need, pay per use basis through web-based tools and applications, as opposed to a direct connection to a server. Data sharing is made possible via cloud computing, which can increase the user's efficiency and output. Nonetheless, there are numerous privacy and security flaws in the Cloud that prevent its widespread use for collaborative purposes. As a result, there is a need for data owners to have some say over what happens to their data once it has been made available to data consumers, in addition to a need for their data to remain private & secure in the Cloud. Key management, security assaults, & data-owner access control are three of the most pressing problems with cloud-based information exchange. When it comes to key management, encryption of data before putting it into the Cloud is essential for keeping sensitive information secret.

Keywords - Cloud Computing, Key Management, Security, Protocol

----------X----------

INTRODUCTION

Due to the distributed nature of the computing, the work being done on multiple computers can be allocated or collected on a single stage of limited stages as opposed to across many stages, and then easily accessed from the specific computer. Hundreds, if not thousands, of different data-registration systems are likely in use by any organization. To grow to a large number of frameworks & large amount of storage, however, distributed computing is the optimum stage. The cloud's pliability extends to its storage options as well. Clients may rapidly scale up or down their processing resources as needed, and when those resources are no longer needed, they can repurpose them in novel ways to produce brand new resources. Through the use of distributed computing, one could obtain the most advantageous stage of provisioning for their asset. Upgrades to the system's assets, such as additional frameworks, capacity of handling, programming, & data storage, can be purchased by clients. In a nutshell, it's the optimal setting in which to share your resources with others. In distributed computing, the adaptability of resources is a major selling point. With this flexibility, the client can adjust the number of processing resources up or down depending on their requirements. Capacity limits can be raised, transformed, etc., with their help. The standard of registering property is always understood. However, it might be difficult to anticipate requirements, especially when requests are volatile. The flexibility & efficiency of distributed computing have been praised. Information cannot be safeguarded from open mists if it is not demonstrated. Always & without fail, the main roadblock for distributed computing is security, both in terms of preventing outside threats and ensuring trustworthy agreeability standards. The term "distributed computing" refers to a paradigm shift in how computing resources are made available online, with the advent of "computing as a service" platforms.

SECURE DATA SHARING IN CLOUD

Data sharing in the cloud is an important area of research because handling data is highly sensitive. The data sharing provides numerous benefits to healthcare industries, engineering industries, institutions, academicians etc. Sharing the secret data between the users is a highly complicated task which involves a high degree of insecurity.

Figure 1 represents the flow diagram of the data sharing in the cloud infrastructure. The cloud server authenticates the user‘s credentials. If the user is unauthentic, the request to access the data is rejected. If the user is authentic, the key is given to the user. The user then retrieves the encrypted file and uses the key to decrypt the encrypted file. Therefore, only a valid user can access the information in the cloud while other users are blocked.

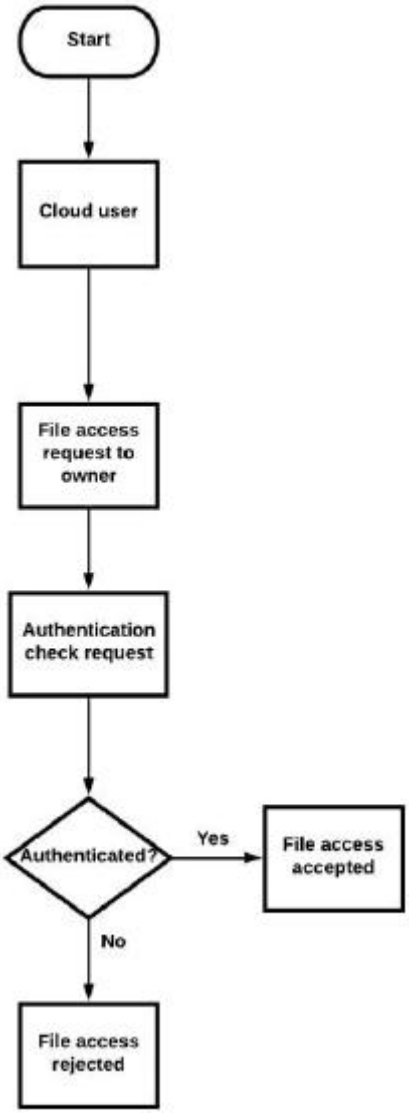


Figure 1: Data Sharing in Cloud

Group Key Management (GKM) is an essential part of cloud-based data sharing. When it comes to ensuring the safety & dependability of group communication, GKM plays a crucial role. When a group of people are sharing data on the cloud, everyone must be certain that their data is safe (Danan et al. 2017). The Cloud Data Owner (CDO) must be able to specify the group which can share the data. The users must be authenticated before accessing the cloud. It must be possible for the CDO to add or remove users from the group. For ensuring the security of data, CDO encrypts the data before storing it in the cloud. Only authorized users can access the encrypted data using the group key provided by the CDO by which confidentiality of data is ensured. The integrity of cloud data should also be ensured so that a cloud user is satisfied in outsourcing the data to the cloud.

uthentication

Only the authentic user must be provided access to the data. Hence, user authentication plays a central role in secure communication for cloud. It verifies the legitimacy of the user before allowing the access to cloud resources. Various methods of authentication are available in literature (Huma Farooq 2017) namely, Username and password authentication, multi-factor authentication, Single Sign On (SSO), Mobile Trusted Module (MTM), Public Key Infrastructure (PKI), and biometric authentication. Reddy *et al*. (2016) classifies the authentication methods based on Password, Smart card and Biometric keys. Each of these methods is susceptible to some form of attack. Therefore, a robust authentication mechanism must be selected depending on the context of the usage.

Confidentiality

Secure data sharing in the cloud environment involves transfer of data in a confidential, flexible and efficient way to other users. Generating secret key and encrypting the data before sharing with the cloud users is an important task. Hence efficient key management and encryption schemes are required.

Data Integrity

Another aspect of secure data sharing namely data integrity assures that the data remains intact without any modification by any unauthorized users. This is really a big challenge for the cloud users because the tenure of the data stored in the cloud varies from a short duration to a very long time. Moreover, a cloud user outsources the data to the cloud provider and hence there is a chance of the data getting modified or corrupted (Shucheng Yu *et al.* 2012). The user cannot rely on the cloud provider for integrity checking. Another requirement for integrity checking is that the verification should be timely. Moreover, the user may not have enough resources for integrity checking by themselves. Therefore, integrity verification can be entrusted to a Third Party Auditor (TPA). Solution for Integrity verification falls into the following schemes (Renuka*et al*. 2014):

MAC based solutions: In this scheme, the file to be stored is divided into blocks and MAC code is generated for each block by the Data Owner, TPA or the cloud provider. While verifying the user or the TPA generates the MAC and verifies if it is valid.

Public Auditing: Here, the user generates the necessary parameters and generates the code for verification and uploads the file to the cloud and sends the verification code to the TPA. During Verification TPA challenges the cloud to check whether the data is held by the cloud. On receiving the challenge the cloud calculates the necessary metadata and passes it to the TPA. TPA verifies the metadata with the verification code provided by the user.

Digital Signature: The digital signature method is used for integrity checking. Depending on the sensitivity of the data, tenure of data storage and frequency of data updation, the integrity scheme can be selected. For cloud data sharing to be useful,

concerns including authentication, privacy, integrity, & key management must be resolved.

KEY MANAGEMENT

Cryptography is the science of transmitting and receiving information securely through a public channel (Dananet *al.* 2017). Cryptography relies on two components namely algorithm, key. Algorithm is the mathematical formulation which when applied encrypts the given information with the help of a key, which is a parameter used by the algorithm for encrypting the data (Jianshen*et al*. 2018). The algorithm part of cryptography consists of encryption, which converts the plaintext to be transmitted into cipher text and decryption which converts cipher text to plaintext.

Just as encryption is central to computer security, the generation and sharing of a cryptographic key is central to encryption. Unlike encryption algorithms, which can be difficult to break, the cryptographic key is a central point of attack which is easy to break. A hacker who obtains the cryptographic key for an encrypted file or session has complete access to the information contained therein. Therefore the key (and its handling) must be made as strong as possible. The creation and sharing of strong keys is a critical part of a secure system, and failure to perform either task well determines the ultimate security of the system. Key management becomes a vital task and it consists of key generation, updating, distribution and deletion of keys. When it comes to a group oriented application group keys are used for sharing of common information and session keys are used for exchanging of information between two parties. Group Key Management (GKM) plays the role in group key generation, updation, distribution and deletion.

CLOUD DATA BASED SHARING

We use a very basic private and secure Cloud data sharing system to illustrate the issues with this type of collaboration. Let's start with a very basic case: a data owner saves some data contents (say, a document) in a cloud service like Google Drive, and then shares it with certain data consumers (e.g., workplace colleagues). The fundamental architecture of Cloud data sharing is depicted in Figure 2 below.

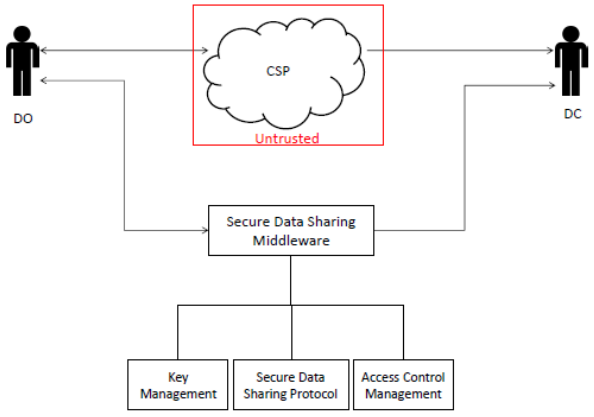


Figure 2: Structure of Cloud-Based Data Sharing

Throughout our thesis, we develop solutions within the Key Management, Secure Data Sharing and Access Control components.

- CSP stands for "Cloud Service Provider," an unreliable company that stores data on its servers.
- Data-sharing middleware refers to the safeguards put in place to preserve the confidentiality and integrity of shared information. Key Management, Secure Data Sharing, & Access Control are the 3 subcomponents that make up the middleware.
- Key Management is in charge of handling all of the encryption keys.
- Safe data transfer is achieved by employing either software or hardware-based procedures to ensure the data's integrity at all times.
- Access Control: Makes sure the information is utilized in accordance with the owner's guidelines.
- "DO" stands for "Data Owner," the person or organization in charge of creating and disseminating data. The DO keeps the encrypted information in the CSP, while the keys to decrypt it are kept in the Key Management system. The DO has complete control over who is allowed to view the information.
- DC: Authorized Data Consumer seeking access to data owned by the DO. The data contents are downloaded from the CSP & associated encryption keys are downloaded from Key Management, and then the DC decrypts the data locally on their machine.

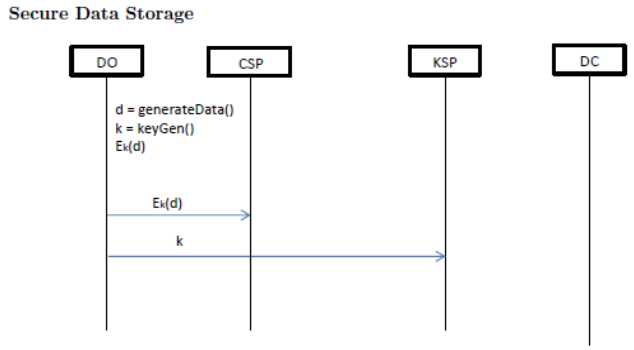
OPERATIONS OF KEY MANAGEMENT

There are five main operations that comprise key management:

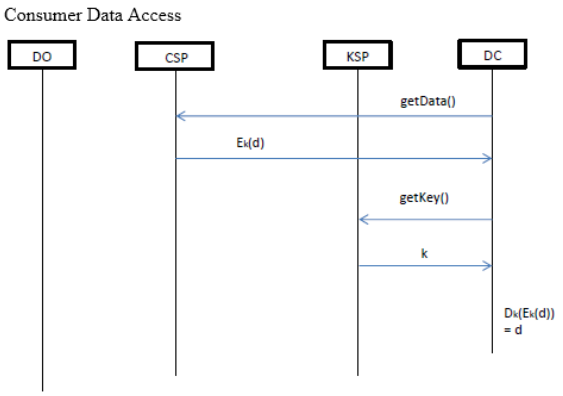
- Key Generation Examining who and how keys are generated. For instance, consumers, trusted key providers, & multiple Cloud Service Providers may all require newly generated keys.
- Key Distribution explains how the necessary entities receive their respective keys. Keys must be disseminated through trusted channels to avoid sensitive information from falling into the wrong hands.
- Key Storage - Where the keys are kept. Where do the keys reside? In the Cloud provider's database, at a reliable key provider, or on the data owner's local machine? It's crucial that keys are kept safe from being misplaced, stolen, or altered. Securing keys & making duplicates to spread them across systems is standard procedure to avoid losing sensitive information.

- Key Revocation, Data owners can remove their consumers' access to their data through a procedure known as "key revocation," which involves either physically removing the consumer's key or rendering it worthless.
- Key Update explains the process by which keys are periodically renewed & upgraded to prevent key disclosure. Changing the key could necessitate re-encrypting all of the data, which would be time-consuming & expensive for the data owner.

PROTOCOL FOR SECURE DATA SHARING



Data & encryption keys are initially created by the DO. The data that the DO wishes to store in the Cloud must first be encrypted on their local PC. Once the data has been encrypted, it is delivered to the CSP for storage, while the encryption keys are sent to a reliable key service provider. Please be aware that the contents of the saved data remain unreadable because the untrusted CSP does not have access to the encryption keys.



Once the DC has verified that it has access to the DO's data, it can retrieve the encrypted data from the cloud. The DC can get the key from the reliable source in a protected & secure manner using encrypted channels of communication (e.g., over the phone, in person, etc.). With this key in hand, the DC may read the entire plaintext of the data.

CONTROL OF ACCESS BY DATA OWNER

When information leaves the limits of a user's local workstation and enters the Cloud, it is no longer under the owner's complete control. Methods now used [B. Qing-hai et al. 2011] to reclaim some measure of access control include, but are not limited to:

- The Access Control Matrix is a two-dimensional representation of who has access to which data and what operations can be performed on that data.

	D1	D2	D3
Bob	R	W	RWD
Alice		RW	R
Dave			W

R stands for Read, W for Write, and D for Delete in the above table.

- **ACLs (Access Control Lists):** When using an ACL, data objects keep track of which users have access to the data & what actions those users are allowed to do. The usage of access control lists (ACLs) is commonplace.

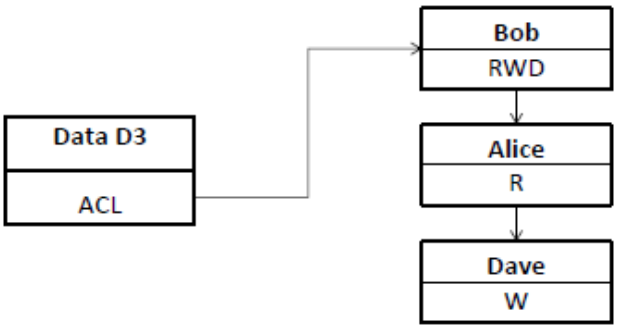


Figure 3: Access Control List

Figure 3 shows an example of a basic access control list for the D3 data set. Bob has full literacy; he can read, write, and delete; Alice & Dave both have limited capabilities.

- **Access Control Capability Lists (ACCL):** the inverse of ACL, where the subject keeps track of data objects & activities they are permitted to carry out on them.

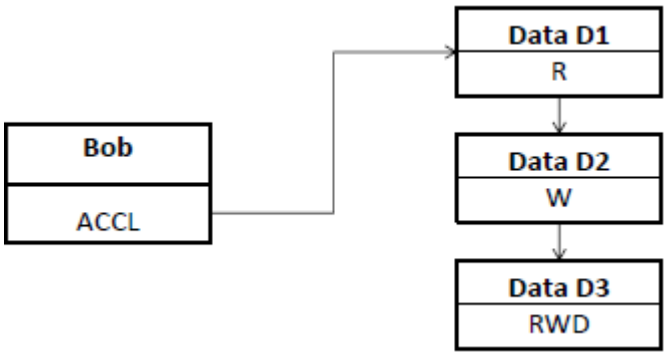


Figure 4: Access Control Capability List

A sample access control list (ACCL) for Bob is shown in Figure 4. It details the operations that can be performed on each of the three data contents (D1, D2, & D3).

- **Role-Based Access Control (RBAC):** like ACLs, RBAC uses roles to assign users to specific levels of access. As an illustration, a manager would have more privileges than an employee would.
- **Attribute-Based Encryption (ABE):** offers finer-grained access control than the preceding. The user's data or private key is where attributes are kept. A data's permissibility for access is determined by the policy's qualities, which are strictly enforced by an access control policy.

Access Control Matrices, Access Control Lists, and Access Control Grant Lists (ACLs, ACCLs, and their variants) are all simple to initiate and can be used to restrict the data's intended usage. However, it can be challenging to manage tens of thousands of themes. In particular if there will be frequent updates to permissions. This is simplified by RBAC since subjects with similar characteristics, including department, can be assigned to the same set of roles. As a result, by modifying the permissions for a single role, access can be restricted for a variety of subjects. It might get tricky, though, if a subject needs access beyond what their role calls for (s). Although ABE, like RBAC, makes use of attributes, once those attributes have been given to a user via a private key, they cannot be modified without resetting the private key's associated authorization token. Due to ABE's encryption, it is best suited for information that is transferred via the Cloud.

CHALLENGES OF SECURE DATA SHARING

Key Management Issues

When a data consumer's access is revoked, the trivial solution to key sharing requires the data owner to re-encrypt the data & redistribute the encryption keys to all members of the group.

We talked about existing methods that try to address these problems, but many of them put more work on the data owner or require trusting the CSP to keep the encryption key secret by revealing it to it. The suggested methods typically suffer from performance concerns, especially when it comes to re-encryption.

- Because of poor handling of encrypted keys.
- There is almost no consideration given to private sharing among thousands or tens of thousands of people.
- It is common practice to entrust CSPs with secret data, which is a potentially dangerous assumption.
- A key management system for sharing data that is easy for the data owner.

Challenges to Secure Data Sharing Protocols

Many people are reluctant to trust their sensitive information to the Cloud because of security concerns. As was previously mentioned, insider assaults remain the greatest risk because insiders have unlimited & direct access to the data. While this simple fix is effective in warding off insider threats, it offers nothing to protect sensitive data stored in the cloud from collusion attacks in which users collude with bad actors to steal private information. In addition, data encryption is a prerequisite for any kind of data exchange in the Cloud. The consequences of a data breach are enormous. Attackers will constantly look for the weakest link to exploit. As a result, one of the greatest difficulties is making sure data is secure at all times and only accessible to those who are authorized to see it.

- Because insiders have unfettered access to data, one of the biggest problems is insider attacks.
- Attacks including collusion on the part of Cloud users and administrators.
- Common security threats include: Man-in-the-middle attacks, sniffing attacks, etc.

Access Control Challenges

Although the data owner is granted granular control over who can access the data and what operations could be performed on it, this is still only partially the case due to the limitations of access control matrices, access control lists, access control classification levels, role-based access control, & attribute-based access. With the explosion in popularity of cloud storage services in recent years, there has been a corresponding rise in the expectation that users will have granular control over who may view & modify their data. Malicious insiders, for example, can access any and all of the data belonging to the data owner. Furthermore, authorized data consumers with read/write access can duplicate the data & share it with others, such as by email attachments or USB transfer, without the data owner's knowledge or consent. Once the information has been downloaded to a user's computer, they are free to do whatever they like with it. Despite the growing demand for data sharing on the Cloud, relatively little has been done in the

existing body of research to meet this demand from the data owner.

Therefore, the key problems are:

- Not granular enough;
- A lack of study into how to stop authorized data consumers from sending each other files via email, USB, etc. without permission.
- Once in possession of the data, the data consumer can do whatever they want with it, and it will be tough to hold them liable.

CONCLUSION

Clouds can also be classified based upon the underlying infrastructure deployment model as Public, Private, Community, or Hybrid clouds. Cloud service providers to implement secure key management protocols. It has been established, however, that there are still problems with key management that undermine trust in Cloud computing. In addition to encrypting and decrypting, key management also includes all the other operations that can be performed on a key, such as creating and deleting keys, activating and deactivating them, moving & storing them, and so on. For the most part, CSPs will encrypt user data using a simple key encryption approach, or they will let users handle encryption themselves.

REFERENCES

1. Arockiam, L &Monikandan, S 2013, „Data security and privacy in cloud storage using hybrid symmetric encryption algorithm", International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 8, pp. 3064-3070.
2. Arora, R, Parashar, A & Transforming CCI 2013, „Secure user data in cloud computing using encryption algorithms", International Journal of Engineering Research and Applications, vol. 3, no. 4, pp. 1922-1926.
3. Arsanjani, A 2004, ‗Service-oriented modeling and architecture', IBM Developer Works, pp.1-15.
4. Asus eee pad transformer prime tf201. . URL http://www:asus:com/Eee/Eee Pad/ Eee Pad Transformer Prime TF201/. Accessed: 22-12-2012.
5. Attila Kertesz (2014), "Characterizing Cloud Federation Approaches", Cloud Computing, Springer International Publishing, pp. 277-296.
6. Au2eu. AU2EU Website, . URL http://www:au2eu:eu/. Accessed: 19-05-2016.
7. Ayesha Kanwal, Rahat Masood and Muhammad AwaisShibli (2014), "Evaluation and Establishment of Trust in Cloud Federation", Proceedings of the International Conference on Ubiquitous Information Management and Communication, Article. No. 12, pp. 1-8.
8. Ayyash M 2016, Coexistence of WiFi and Li-Fi toward 5G: concepts, opportunities, and challenges, IEEE Communication Magazine, vol. 54, no. 2, pp. 64-71.
9. B. Blanchet. Automatic veri_cation of correspondences for security protocols. Journal of Computer Security, 17(4):363{434, 2013.
10. B. Li. Research and application of soa standards in the integration on web services. Education Technology and Computer Science (ETCS), 2010 Second International Workshop on, 2:492{495, 2010. doi: 10:1109/ETCS:2010:199.
11. B. M. Silva, J. J. Rodrigues, F. Canelo, I. C. Lopes, and L. Zhou. A data encryption solution for mobile health apps in cooperation environments. J Med Internet Res, 15(4):e66, 2013.
12. B. Qing-hai and Z. Ying. Study on the access control model. 1:830{834, July 2011. doi: 10:1109/CSQRWC:2011:6037079.
13. Baktır, A. C., Ahat, B., Aras, N., Özgövde, A. and Ersoy, C. (2019), "SLA-aware optimal resource allocation for serviceoriented networks", Future Generation Computer Systems, Vol.101, pp. 959-974.
14. Barsoum, AF &Hasan, A 2013, „Enabling dynamic data and indirect mutual trust for cloud computing storage systems", IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 12, pp. 2375-2385.
15. Baumgart, I., Heep, B. and Krause, S. (2007), "OverSim: A flexible overlay network simulation framework", In IEEE global internet symposium, DOI:10.1109/GI.2007.4301435 .
16. Bens Paramean, and Rizal Ricky Rumanda (2011), "Integrated model of cloud-based E-medical record for health care organizations", Proceedings of the 10th WSEAS international conference on E-Activities, pp. 157-162.
17. Bhaskar, M &Umadevi, G 2015, „Public auditing For shared data with efficient user revocation in the cloud", International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), vol. 16, no. 2, pp. 39-42.
18. Binns, J. M., Ulness, L. C., Knowler, J. E., Waggoner, C. B. F., Backman, T. K., Barnard, J. B. and Bordenet, M. J. (2019), U.S. Patent Application No. 10/305,721.
19. Bluetooth Technology Web Site. URL http://www:bluetooth:com/Pages/Bluetooth-Home:aspx. Accessed: 12-01-2013.

20. Boddy, A., Hurst, W., Mackay, M., El Rhalibi, A., Baker, T. and Montañez, C. A. C. (2019), "An Investigation into Healthcare- Data Patterns" Future Internet, Vol.11, No. 2, pp. 30.
21. George, RS &Sabitha, S 2013, „Survey on data integrity in cloud computing", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, no. 1, pp. 123 - 125.
22. Kant, DC & Sharma, Y 2013, „Enhanced security architecture for cloud data security", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, pp. 571-575.

Corresponding Author

Saket Nigam*

Research Scholar, Shri Krishna University, Chhatarpur M.P.