iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VII **Month of publication:** July 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

[1]B. Pavan Kumar, [2]Prof. GVNKV Subba Rao

[1]*M.Tech (CS) Student,* [2]*Vice Principle & HOD of CSE*
[1,2]*Sree Dattha Institute of Engineering and Science, Hyderabad.*

Abstract: ***Cloud computing is renowned as an alternative to Traditional information technology due to its inherent resource-sharing and low-maintenance characteristics. With the nature of low preservation, cloud computing provides an inexpensive and capable elucidation for giving out group resource among cloud users. Unfortunately, sharing data in a multi-owner approach while preserving data and identity privacy from an untrusted cloud is still a challenging issue; due to the recurrent alter of the membership. In this paper, we propose a safe and sound multiowner data sharing scheme, for dynamic groups in the cloud. By leveraging group signature and active broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.***

Key Words: Data sharing, multiowner, resource sharing, Cloud computing, encryption techniques

1. INTRODUCTION

In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. Cloud computing is one of the greatest platform which provides storage of data in very lower cost and available for all time over the internet Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and devices on demand. Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage.

Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues. CS2 provides security against the cloud provider, clients are still able not only to efficiently access their data through a search interface but also to add and delete files securely. Several security schemes for data sharing on untrusted servers have been proposed secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase.

IJRASET: ISSN: 2321-9653

2. LITERATURE SURVEY

E. Goh, H. Shacham, N. Modadugu, and D. Boneh [4] the use of SiRiUS is compelling in situations where users have no control over the file server (such as Yahoo! Briefcase or the P2P file storage provided by Farsite). They believe that SiRiUS is the most that can be done to secure an existing network file system without changing the file server or file system protocol. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction. B. Wang, B. Li, and H. Li, [5] in this paper, we propose Knox, a privacy-preserving auditing scheme for shared data with large groups in the cloud. They utilize group signatures to compute verification information on shared data, so that the TPA is able to audit the correctness of shared data, but cannot reveal the identity o f the signer on each block. With the group manager's private key, the original user can efficiently add new users to the group and disclose the identities of signers on all blocks. The efficiency of Knox is not affected by the number of users in the group

3. RELATED WORK

In [4], Kallahalla et al. proposed a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. By dividing files into file groups and encrypting each filegroup with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation. In [5], files stored on the untrusted server include two parts: file metadata and file data. The file metadata implies the access control information including a series of encrypted key blocks, each of which is encrypted under the public key of authorized users. Thus, the size of the file metadata is proportional to the number of authorized users. The user revocation in the scheme is an intractable issue especially for large-scale sharing, since the file metadata needs to be updated. In their extension version, the NNL construction [10] is used for efficient key revocation. However, when a new user joins the group, the private key of each user in an NNL system needs to be recomputed, which may limit the application for dynamic groups. Another concern is that the computation overhead of encryption linearly increases with the sharing scale. From the above analysis, we can observe that how to securely share data files in a multiple-owner manner for dynamic groups while preserving identity privacy from an untrusted cloud remains to be a challenging issue. In this paper, we propose a novel Mona protocol for secure data sharing in cloud computing. Compared with the existing works, it offers unique features which are listed in proposed work.

4. PROPOSED WORK

To achieve secure data sharing for dynamic groups in the cloud, we expect to combine the group signature and dynamic broadcast encryption techniques. Specially, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users. Unfortunately, each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the ciphertext increase with the number of revoked users. Thus, the heavy overhead and large ciphertext size may hinder the adoption of the broadcast encryption scheme to capacity-limited users. To tackle this challenging issue, we let the group manager compute the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the ciphertext size. Specially, the computation overhead of users for encryption operations and the ciphertext size are constant and independent of the revocation users.

First, the key escrow problem is resolved by a key issuing protocol that exploits the characteristic of the data sharing system architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data-storing center with their own master secrets. The 2PC protocol deters them from obtaining any master secret information of each other such that none of them could generate the whole set

IJRASET: ISSN: 2321-9653

ISSN: 2321-9653

of user keys alone. Thus, users are not required to fully trust the KGC and the data storing center in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious KGC or data-storing center in the proposed scheme. Second, the immediate user revocation can be done via the proxy encryption mechanism together with the CP-ABE algorithm. Attribute group keys are selectively distributed to the valid users in each attribute group, which then are used to re-encrypt the cipher text encrypted under the CPABE algorithm. The immediate user revocation enhances the

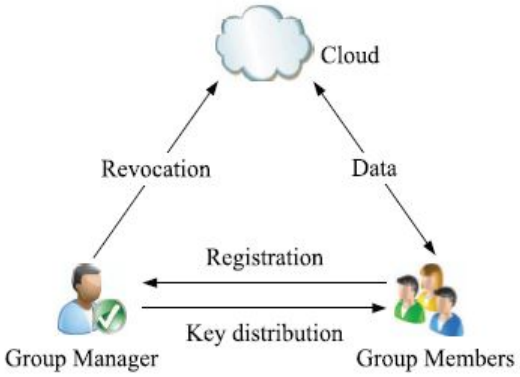


Fig.1. System Model

Backward or forward secrecy of the data on any membership changes. In addition, as the user revocation can be done on each attribute level rather than on system level, more fine grained user access control can be possible. Even if a user is revoked from some attribute groups, he would still be able to decrypt the shared data as long as the other attributes that he holds satisfy the access policy of the cipher text. Data owners need not be concerned about defining any access policy for users, but just need to define only the access policy for attributes as in the previous ABE schemes. The proposed scheme delegates most laborious tasks of membership management and user revocation to the data storing center while the KGC is responsible for the attribute key management as in the previous CP-ABE schemes without leaking any confidential information to the other parties. Therefore, the proposed scheme is the most suitable for the data sharing scenarios where users encrypt the data only once and upload it to the data-storing centers, and leave the rest of the tasks to the data-storing centers such as re-encryption and revocation.

- Our contributions to solve the challenges presented above, a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions of this paper include:
- Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users.
- We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.
- We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

5. DESCRIPTION OF SYSTEM

The proposed systems in comprised of the concepts

- ✓ System Model
- ✓ Group Signature
- ✓ Dynamic Broadcast Encryption
- ✓ User Revocation
- ✓ File Access and File Deletion
- ✓ Traceability

System Model:

Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to, we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

IJRASET: ISSN: 2321-9653

Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. Therefore, we assume that the group manager is fully trusted by the other parties.

Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In our example, the staffs play the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company.

Group Signature:

The concept of group signatures was first introduced in by Chaum and van Heyst. In general, a group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability. In this paper, a variant of the short group signature scheme will be used to achieve anonymous access control, as it supports efficient membership revocation.

Dynamic Broadcast Encryption:

Broadcast encryption enables a broadcaster to transmit encrypted data to a set of users so that only a privileged subset of users can decrypt the data. Besides the above characteristics, dynamic broadcast encryption also allows the group manager to dynamically include new members while preserving previously computed information, i.e., user decryption keys need not be recomputed, the morphology and size of cipher texts are unchanged and the group encryption key requires no modification. The first formal definition and construction of dynamic broadcast encryption are introduced based on the bilinear pairing technique in, which will be used as the basis for file sharing in dynamic groups.

User Revocation:

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users. As illustrated in Table 1, the revocation list is characterized by a series of time stamps. Let ID group denote the group identity. The tuple represents that user i with the partial private key is revoked at time are calculated by the group manager with the private secret.

File Access and File Deletion:

Getting the data file and the revocation list from the cloud server. In this operation, the user first adopts its private key to compute a signature sigma u on the message by using Algorithm 1, where t denote the current time, and the IDdata can be obtained from the local shared file list maintained by the manager. Then, the user sends a data request containing to the cloud server. Upon receiving the request, the cloud server employs Algorithm 2 to check the validity of the signature and performs revocation verification with Algorithm 3 if necessary according to the revocation list. After a successful verification, the cloud server responds the corresponding data file and the revocation list to the user. File stored in the cloud can be deleted by either the group manager or the data owner.

Traceability:

When a data dispute occurs, the tracing operation is performed by the group manager to identify the real identity of the data owner.

6. SIMULATION

File Generation and Deletion

To store and share a data file in the cloud, a group member performs the following operations:

1. Getting the revocation list from the cloud. In this step, the member sends the group identity IDgroup as a request to the cloud. Then, the cloud responds the revocation list RL to the member.
2. Verifying the validity of the received revocation list. First, checking whether the marked date is fresh. Second, verifying the contained signature. Revocation list is invalid, the data owner stops this scheme.
3. Encrypting the data file M. This encryption process can be divided into two cases according to the revocation list.

IJRASET: ISSN: 2321-9653

ISSN: 2321-9653

a. **Case 1.** *There is no revoked user in the revocation list:*

i. Selecting a unique data file identity ID_{data};
ii. Choosing a random number $k \in Z_q^*$;
iii. Computing the parameters C_1, C_2, K, C as the following equation:

$$\begin{cases} C_1 = k \cdot Y \in G_1 \\ C_2 = k \cdot P \in G_1 \\ K = Z^k \in G_2 \\ C = Enc_K(M). \end{cases} \quad (3)$$

b. **Case 2.** *There are r revoked users in the revocation list.*

i. Selecting a unique data file identity ID_{data};
ii. Choosing a random number $k \in Z_q^*$;
iii. Computing the parameters C_1, C_2, K, C as the following equation:

$$\begin{cases} C_1 = k \cdot Y \in G_1 \\ C_2 = k \cdot P_r \in G_1 \\ K = Z_r^k \in G_2 \\ C = Enc_K(M). \end{cases} \quad (4)$$

In (4), Z_r and P_r are directly obtained from the revocation list.

To study the performance, we have simulated can done by using C programming language with GMP Library,Miracl Library , and PBC Library. The simulation consists of three components: client side, manager side as well as cloud side. Both client-side and manager-side processes are conducted on a laptop with Core 2 T7250 2.0 GHz, DDR2 800 2G, Ubuntu 10.04 X86. The cloud-side process is implemented on a machine that equipped with Core 2 i3-2350 2.3 GHz, DDR3 1066 2G,Ubuntu 12.04 X64. In the simulation, we choose an elliptic curve with 160-bit group order, which provides a competitive security level with 1,024-bit RSA.

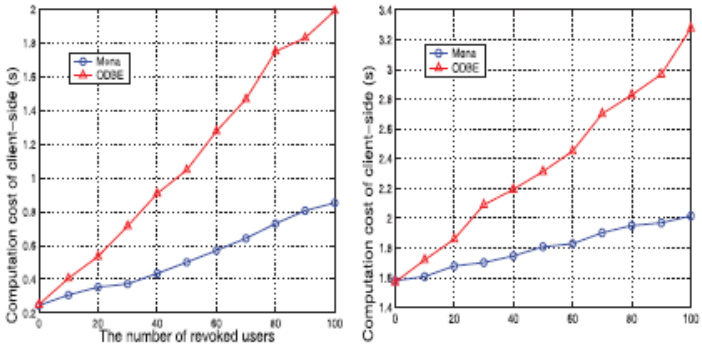
Algorithm (1). Signature Generation
Input: Private key (A, x), system parameter (P, U, V, H, W) and data M.
Output: Generate a valid group signature on M.
begin
Select random numbers $\alpha, \beta, r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2} \in Z_q^*$
Set $\delta_1 = x\alpha$ and $\delta_2 = x\beta$
Computes the following values

$$\begin{cases} T_1 = \alpha \cdot U \\ T_2 = \beta \cdot V \\ T_3 = A_i + (\alpha + \beta) \cdot H \\ R_1 = r_\alpha \cdot U \\ R_2 = r_\beta \cdot V \\ R_3 = e(T_3, P)^{r_x} e(H, W)^{-r_\alpha - r_\beta} e(H, P)^{-r_{\delta_1} - r_{\delta_2}} \\ R_4 = r_x \cdot T_1 - r_{\delta_1} \cdot U \\ R_5 = r_x \cdot T_2 - r_{\delta_2} \cdot V \end{cases}$$

Set $c = f(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$
Construct the following numbers

$$\begin{cases} s_\alpha = r_\alpha + c\alpha \\ s_\beta = r_\beta + c\beta \\ s_x = r_x + cx \\ s_{\delta_1} = r_{\delta_1} + c\delta_1 \\ s_{\delta_2} = r_{\delta_2} + c\delta_2 \end{cases}$$

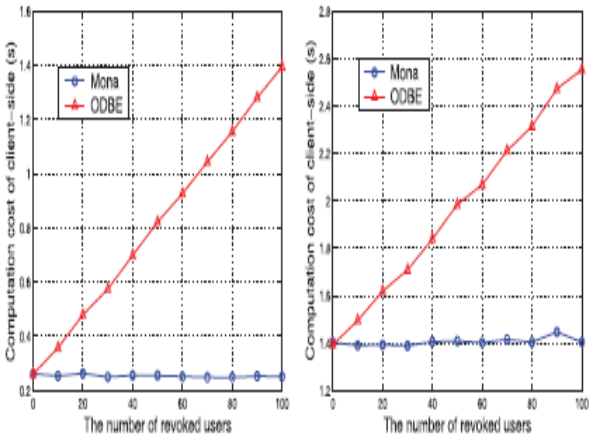
Return $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$
end



(a) Accessing a 10 MB file (b) Accessing a 100 MB file

IJRASET: ISSN: 2321-9653

ISSN: 2321-9653



(a) Generating a 10 MB file (b) Generating a 100 MB file

7. CONCLUSION

In this paper, we design a secure data sharing scheme for dynamic groups in an untrusted cloud. In it a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

8. REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud, IEEE transactions on parallel and distributed systems, vol. 24, no. 6, June 2013.

[2] OASIS, "Business Process Execution Language for Web Services, Version 2.0," 2007.

[3] D. Schall, H.-L. Truong, and S. Dustdar, "Unifying Human and Software Services in Web-Scale Collaborations," IEEE Internet Computing, vol. 12, no. 3, pp. 62-68, May/June 2008.

[4] D. Schall, "Human Interactions in Mixed Systems—Architecture, Protocols, and Algorithms," PhD dissertation, Vienna Univ. of Technology, 2009.

[5] A. Agrawal et al., "WS-BPEL Extension for People (BPEL4People), Version 1.0," 2007.

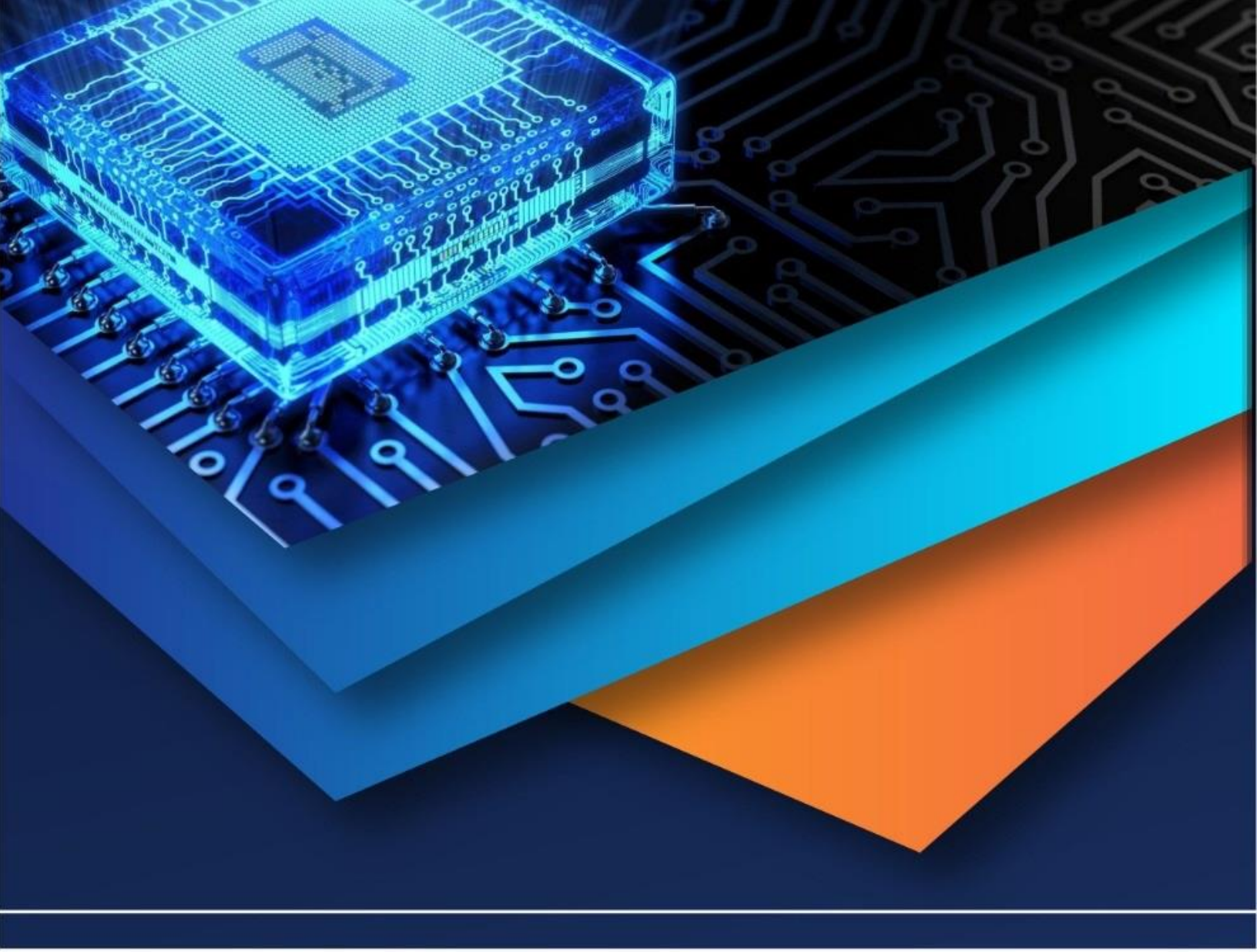
[6] D. Brabham, "Crowdsourcing as a Model for Problem Solving: An Introduction and Cases," Convergence, vol. 14, no. 1, pp. 75-90, 2008.

[7] D. Artz and Y. Gil, "A Survey of Trust in Computer Science and the Semantic Web," J. Web Semantics: Science, Services and Agents on the World Wide Web, vol. 5, no. 2, pp. 58-71, 2007.

IJRASET: ISSN: 2321-9653

B.PAVAN KUMAR pursing M.Tech C.S in Sree Dattha Institute of Engineering and Science, Sheriguda, R.R dist, Telangana, India.

Prof. GVNKV SUBBARAO submitted Thesis in JNTUH. Received M.Tech Degree from JNTU Ananthapur and working as Vice Principle & HOD of CSE in Sree Dattha Institute of Engineering and Science, Sheriguda, RR dist, Telangana, India.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)