Fine-grained Access Control in Distributed Cloud Environment using Trust Valuation Model

Aparna Manikonda[1]
Research Scholar, Department of Computer Science
Nitte Meenakshi Institute of Technology, Karnataka, India

Nalini N[2]
Professor, Department of Computer Science
Nitte Meenakshi Institute of Technology, Karnataka, India

***Abstract*—Cloud computing has been in existence as an adaptable technology that gets integrated with IoT, Big-Data, and WSN to provide reliable, scalable and mesh-free services. However, because of its openness in nature, the privacy of the cloud is an important parameter for today's research. The most important privacy factor in cloud is access control and user trust. Many articles related to access control and trust management were presented, but most of them include highly complex algorithms that result in network overhead. This proposed security framework is for a better and more effective system wherein multiple distributed centers are created with trust-based computing for authentication and validation of requests from users and their resources. The idea of trust here is for efficient decision-making and establishing reliable relationships among users and resources using least computations. Each user has different permissions for each file present in the cloud server. The simulated results shows improvement in the rate of successful transactions, time cost and network overhead.**

***Keywords*—Fine-grained; distributed; access control; trust**

I. Introduction

The security issues like privacy, trust, authentication and authorization need more attention with the rapid advancement in day-to-day technologies. Among them, access control and trust management are critical and complex issues that require more focus. But in the cloud environment, the access control approaches are semi-trusted because of the users snooping nature [1-2] that offer the resource or its attributes a complete access based on the rights of the user. Most of the access management methods [3-7] use encryption and decryption algorithms for protection of legit users. To reduce the computation overheads, many researchers [8-12] used the trust parameter in the process of decision-making for validation and authentication of user and their resources.

The research issues subjected to existing techniques involve the following:

1) The methods related to fine-grained involve lot of mathematical computations.

2) Trust-based involves subjective assignment of weights to the attributes considered for calculation of trust value which leads to time cost, and

3) Centralized-based leads to network overhead.

Hence, the designed model is named as distributed fine-grained access control using trust management (DFGACT). In this work, multiple distribution centers are created for accessing the data by authorized users on basis of their trust values associated with them. Rest of the paper is organized as follows: Section II is literature survey, Section III is proposed approach and Section IV is results and analysis about the proposed approach followed by a conclusion in Section V.

II. Related Work

One of the mostly used cryptographic access control method is designed by Sahai [13] for volatile cloud situations. Many literature papers used CP-ABE and KP-ABE schemes to secure data processing in the cloud and WSN [14-18]. In these methods, the complexity of encryption growth is linear with the count of each attribute and conveys heavy computation overheads. CP-ABE schemes are the most used for fine-grained security in cloud computing. The attribute statistics [19] are completely hidden inside the access policy by way of the use of the randomizable fuzzy approach for decryption purposes. Somchart et al. [20] used the CP-ABE method for mobile cloud environments by way of introducing new proxy encryption to reduce the cost of decryption and encryption for mobile users. But the outsourcing encryption isn't always specified. CP-ABE calls for data proprietors to generate multiple ciphertexts which result in sizable overheads in computation. To triumph over this, an LSSS based CP-ABE has been proposed [21] that can decrypt the records that are relatable with this matched part.

Anil Kumar et al. [22] tried to triumph over the troubles associated with RBAC, where users can access entire object without any further authentication once access is granted by manipulating swift storage. Qian et al. [23] proposed a Merkle tree based on time and attribute that stores private keys of the user for decryption purposes to efficient access of the resources. A lightweight statistical computation [24] is carried out by the cloud server for granting unique access privileges to individual users. However, with the increasing variety of attributes the overhead increases.

The large statistics are stored specifically in the cloud for controlling the access of a massive amount of data with closed permissions of individual users [25]. However, this scheme hides total attributes of a user for getting an entry pass to the access rights. The conventional cloud storage structures goes through a hassle of returning the incorrect seek consequences or not going back to the total seek results, this can be solved by using the applied decentralized system model with the cipher textual content-based key-word seek characteristic according to the smart reduced in size Ethereum blockchain [26].

Qi Li et al. [27] constructed a scheme named SEMAAC for mHealth applications that have IoT enabled to achieve the functions of de-centralization. Here, each CSP computes the decryption costs by interacting with Associated Authority. But, the verification time of each PDC increases linearly with the number of associated authorities. For a specific biological system of healthcare industry in cloud computing [28] the user's closed permissions are mixed with fog computing to provide high-level security.

Roy et al. [29] constructed a concept in the direction of transportable cloud computing for the healthcare industry. This portable cloud display helps in analyzing the statistics with recognition of the patients' records and in removing proposals in medicinal services programs. A dynamic authorized system was proposed for cloud computing [30] where the authorized users are identified based on trust value. The access privileges of these users are created on their behaviour with the system. However, this work adds an overhead due to its various assignments and removal of permissions for malicious users.

III. Proposed Work

There are three important issues while accessing data from the server. Firstly, users having access to servers may additionally try and access data that isn't always intended for them. To keep away from such problems, every user needs to have a particular privilege to access the server. Secondly, Trust is an important parameter for improving the relationship between the user and their resources. Thirdly, a maximum of the theories mentioned for improving safety features are liable to a single point of failure. However, the decentralized version has higher throughput and lower fees together with overcoming the failure of single-factor issues within the system as compared to the traditional cloud storage device.

The main idea behind this research is to eliminate the complex computations that are involved in the existing state of art methods. The novelty behind this access-control method lies in the combination of 1) Decentralized approach to avoid single-point failures 2) Fine-grained approach for unique privileges for users and 3) Trust for an effective authorization process. Although many methods related to the above discussed issues are existing but none of the techniques is a combination of these three tactics. The reason to combine these three tactics is for better time cost, success rate and reduction of network overhead.

This phase of work defines a simplification of the proposed scheme DFGACT. Requirements in this approach are:

1) Multiple VMS of cloud that acts as a distribution center for the scheme.

2) Each DC has a cloud service provider that takes care of the incoming requests from the user and owner of the file/resource.

3) The distribution center stores the consumer/User information, trust matrices and permission table of the resource.

4) Each file has a permission table, the owners of the file/ resource decide on the permissions that a user/consumer should have and accordingly receives the PID of the file/resource that authorize them to access records.

Here, the user/consumer request is processed through these modules as shown in Fig. 1 to undergo the authorization and authentication system. The consumer request is of the form (UID, PID, RID, Trust value). The representation for the same is given in the table 1. To gain access control, the method used an idea similar to [31]. The access policy is a fine-grained in nature; this combines three methodologies RBAC, ARL and ABAC. For fine-grained precision, a set of access rules is assigned to each user that defines the access rights of that resource/file. In the proposed case, each file has a set of permissions in the form of attributes. The values associated with the attribute decide the right to access the resource/file. Every file/resource and a unique permission ID has been assigned to the user based on the initial demand/request. No two users can have the same permission ID for that resource.

However, the uniqueness of the work is addition of distribution centers that distributes trust matrices among neighboring CSPs for identification of valid users to avoid malicious requests for a better network overhead. Besides, trust computing is taken into consideration as a measurable factor in the scheme that considers users trust credentials and computing power of resources for better success rate. Table I describes the notations used in the paper.

TABLE I. Notations

Sl.no.	Notation	Meaning
1	**AC**	Authorization Centre
2	**DC**	Distribution Centre
3	**DO**	Data Owner
4	**CNM**	Data Consumer
5	**ALC**	Access level code or permission IDs
6	**CSP**	Cloud service provider
8	C_a	Type of user
9	C_t	Authentication degree
10	TT_{VAL}	Total Trust value
11	T_{THRSD}	Trust threshold
12	M	Unique code in the permission table
13	N	Set of permissions associated with FILE
14	Z	File name
15	RQ	Degree of request potentiality
16	r	Priority of current request and is decided by CSP of DC
17	RQ_f	Number of times the user requested for the resource
18	RQ_s	Degree of valid request.
19	R_{id}	Request ID
20	(U_{id})	USER ID
21	P_{id}	Permission ID
22	(F_{id})	FILE ID

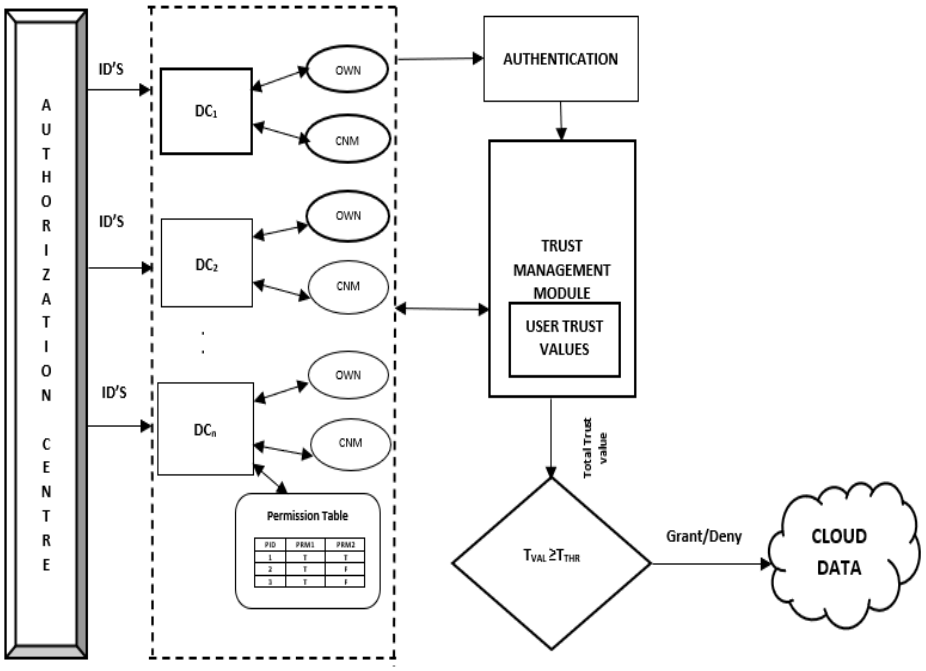

Fig. 1. System Architecture of DFGACT.

The scheme starts with an authentication procedure which involves the verification of user identity by its necessary associated credentials, such as User-Id, password, and RSA token. For the valid user, the activity is been recorded by the system in a log file for future reference. The request gets dropped for an invalid user and the information about the same is sent to remaining distribution centers. Followed by an authorization procedure, where the DC extracts the permission ID of the resource from the user request and assign the data to client according to the permissions associated with the F_{id} (P_{id}).

A. System Architecture

The proposed architecture distributed fine-grained access control with trust computing named DFGACT includes a trust management module and an access control module in conjunction with four entities as shown in Fig. 1. The entities are Authorization center (AC), Distribution Center (DC), Data Owner (DO), and Data Consumer (CNM). In the proposed scheme, the consumer can get the right of entry to the resource through the ALC code of the report/ resource. Each of the entities with its functionalities is mentioned as underneath:

USER/Owner: This entity can store or access the information; the one tries to read /write the resource and this must be a valid user before accessing the resource.

CSP: This entity provides services to the authorized users. This resides inside the distribution centre.

Distribution Centre (DC): Each distribution center generates ID'S to user and owner of the resources. This entity stores the permission table of each resource, access policy, information about the owner and consumer. Every distribution center has a CSP provider to validate the authorized users for accessing the resources.

Authorization Centre (AC): Authorization center creates various distribution centers. A unique ID is associated for each distribution center. This entity acts as a database for storing information about the distribution center.

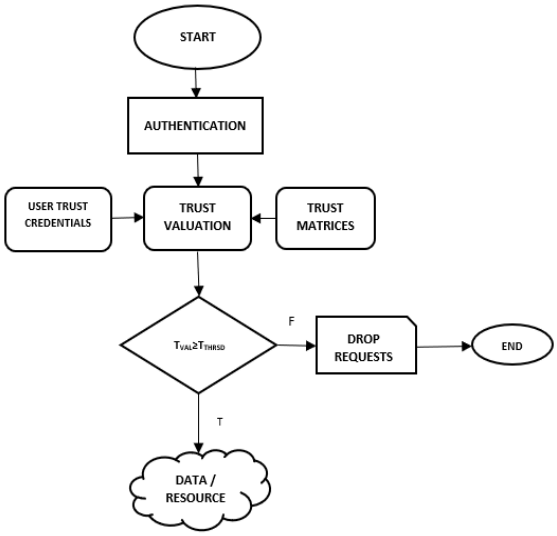

Fig. 2. Flowchart of the Proposed Architecture DFGACT.

The working principle of DFGACT is as under and the flowchart for the same is shown in Fig. 2:

1) Request from USER or Consumer to get entry into the Cloud data or Services through web interface of a specific distribution centre.

2) The distribution centre authenticates every individual via analysing the important related credentials such as $\boldsymbol{C_a}$ to identify the user is a trusted or untrusted. If the $\boldsymbol{C_a}$ are determined legitimate, then the request for access undergo trust evaluation process, or else the request of the consumer is denied for any additional processing.

3) If authentication check fails the CSP in that particular DC's drops the request and transfer the trust information among CSP of different DC's. The trust values of the user are computed by taking the inputs from user trust credentials and trust matrices as shown in Fig. 2. There are three distinct instances for inspection of trust value:

a) Instance 1: Reliable user and Non-reliable user: Here, CSP of each DC authenticates the request based on its frequency and user trust. If $TT_{VAL} < T_{THRSD}$ then CSP of that particular DC drops the request and informs other DC's about the incoming threat.

b) Instance 2: New/Unidentified user: In case of any new or unidentified user, the CSP checks the trust value of the requesting user from its neighboring CSP. The fetched value is added to its own trust matrices.

c) Instance 3: Malicious Attack: CSP keeps track of the requests received at that distribution centre. If any suspicious activity is found then user's trust value is decreased otherwise value of trust increases.

4) For valid requests, CSP of that DC finally allow the subject to use the resource.

B. Evaluation Startegy

The evaluation strategy of this model is setup in three phases: 1) Network phase, 2) Access control strategy and 3) Trust Evaluation strategy.

In the approach, each Distribution Centre has a table that contain trust matrix of each user associated with that DC. For every attempt by the user with the cloud resource, the DC share the trust matrices of that user to its neighboring DCs. The user requests are verified and are either granted or denied to access the service.

1) Network model: The network consists of several Distribution Centers(DC), cloud service providers (CSP), Owners (OWN), and Users(U).

$$DC = \sum_{i=1}^{dc} DC_i \quad \forall\ (1 \le i \le dc) \tag{1}$$

$$CSP = \sum_{i=1}^{csp} CSP_i \quad \forall\ (1 \le i \le csp) \tag{2}$$

$$OWN = \sum_{i=1}^{own} OWN_i \quad \forall\ (1 \le i \le own) \tag{3}$$

$$U = \sum_{i=1}^{n} u_i \quad \forall\ (1 \le i \le n) \tag{4}$$

Every pair of DCs can communicate securely and has a set of disjoint users U which means no two users can belong to same DC, $i, j \in DC$ and therefore is written as $U_i \cap U_j = \emptyset$. The OWN of the resource decides the attribute values of the file, that carries a set of rights to perform a specific task on the resource.

2) Access control strategy: Each file stored has a set of attributes and are named as permissions in this work. The permission values to the file are decided by the owner of the file. The permission ID (PID) uniquely determines the permissions associated with that. Every Distribution Centre in the network assigns the PID to the user according to the service plan.

This approach uses the access policy similar to [31]. Here, the file/resource permissions are arranged in tabular structure with unique permission ID (PID), and its adjacent columns are represented in Boolean format. The permissions for each file are arranged as shown in the Table II.

TABLE II. PERMISSION TABLE OF THE RESOURCE

PID	Read	Write	Edit	Move	Share	Download	Delete
1	1	0	0	0	1	1	1
2	1	1	1	0	0	1	0
3	1	0	0	0	1	1	0
4	1	0	0	1	1	1	0
5	1	0	0	0	0	0	0

Each user is assigned with a unique code to access the resource. Each file will set access limits to requesting user according to permissions from set, and is represented in the equation below:

$$M \rightarrow N \tag{5}$$

Where:

"M" is a unique code in the permission table,

"N" is a set of permissions associated with $\boldsymbol{Z}$.

For e.g., if any user has assigned with PID-4 of that file then no other user can have PID-4 for that resource/file.

3) Trust assessment model: The authorization process of this scheme is depended on trust-based evaluation for an efficient decision making. The users trust value is calculated and is compared with the threshold trust $\boldsymbol{T_{THRSD}}$. After each transaction these trust values gets updated in the database. The value of the trust is related to the CSP of that particular DC in a particular session. For the evaluation of trust, the following parameters has been considered: 1) User interactions with the system C_a, 2) Type of user C, 3) The number of times the user requested for the resource RQ_f, 4) Degree of valid request RQ_s and 5) Estimated computing power of the resource $\boldsymbol{E_{CP}}$.

The Trust matrix is of form $< T_{VAL}, E_{CP} >$ where:

The trust value $\mathbf{T_{VAL}}$ of each user for a particular session is calculated from the equations below:

$$RQ = r \times \frac{RQ_s}{RQ_f} \tag{6}$$

$$RC_{VAL} = C_t \times C_a \times RQ \tag{7}$$

Where:

C_t value increases with valid requests and declines at invalid ones.

C_a value greater than 0.5 is a trusted user and less then 0.5 is invalid or malicious user and equals 0.5 is for new user.

RQ value for degree of request potentiality.

RC_{VAL} handles the type of user and potentiality of the request.

The ongoing limit of a cloud asset influences the exhibition of the cloud supplier and exchange execution. In this manner, the ongoing asset limit boundaries like CPU, RAM, and Network ought to be thought about while assessing trust an incentive for a cloud asset to empower a framework to gauge on the off chance that the asset can execute the expected work or not. Hence, the CPU time of resource is considered as Estimated Computing Power (E_{CP}).

$$E_{CP} = \frac{CPU_{JOB}}{CPU_{RESOURCE}} \quad (8)$$

In this work, the trust value $\boldsymbol{T_{VAL}}$ is calculated from two attributes, the first attribute handles the frequency of the request and type of user. The second attribute handles the computing power of the resource.

$$T_{VAL} = RC_{\boldsymbol{VAL}} + E_{CP} \quad (9)$$

At the end of each transaction from the DC to USER, the trust value T_{VAL} gets updated and broadcasted to the other DC's. The other DC's keeps a record of these values so that there should not be any discrepancies while handling the requests.

Algorithm: Proposed DFGACT

1. **Input:** Parameter associated with calculation of trust value
2. **Output:** Updated Trust Value
3. While(true)
4. User send request (T_{VAL}, E_{CP}) to DC
5. if ($C_t \leq 1$ && $C_a > 0.5$) then
6. if ($T_{VAL} \leq T_{THRSD}$) then
7. Continue with the service;
8. Calculate RQ using eq.6
9. Calculate RC_{VAL} using eq.7
10. else
11. $RQ = RQ - 1$;
12. $C_t = C_t - 1$;
13. end if;
14. Calculate T_{VAL} from eq .9 and update the database with this new value
15. end if;
16. Broadcast (T_{VAL},ECP) to other DC's
17. DC extracts access level permission for the user.
18. *if* (R_{id} (U_{id}) $\rightarrow$ *true* && F_{id}) *then*
19. R_{id} (U_{id}) $\leftarrow$ P_{id} (F_{id})
20. end if ;
21. $RQ_s \leftarrow RQ_s + 1$
22. $RQ_f \leftarrow RQ_f + 1$
23. end while;

IV. Results and Analysis

This paper used a CloudSim3.0 [32] and experiment environment is eclipse editor. The programming language used is java to simulate the proposed method. It is assumed, each VM of the cloud as a Distribution Centre (DC). Likewise, 8 DC's are created for the evaluation of proposed scheme. The scheme evaluates the user's behaviour according to trust management module. At the beginning, trust value of registered users is defined as "0.5". Depending on the successful attempts, the trust value of user keeps changing, but the value should not exceed trust threshold. In this approach trust threshold is assigned as 1. The results of DFGACT and literature [30] are compared thorough simulation. The results are proved that DFGACT has better efficiency than literature [30].

Fig. 3 represents time cost of both the schemes in comparison with no. of users. From the result it can be seen that with the increasing number of users the time cost increases for Mehraj [30]. On the other hand, the DFGACT less delay is because this scheme has simple way of accessing request in fine-grained manner, whereas in Mehraj [30] the conversion of roles into tasks into permissions results in delay at higher cost that increases with the increasing no. of users.

Fig. 4 shows the network traffic rises with the no. of requests for both schemes. However, DFGACT has less overhead in comparison with the other approach. The DFGACT has less overhead as compared to Mehraj [30] because of DFGACT distributed nature. Mehraj [30] has higher overhead because of its centralized approach and at the same time various assignments of roles-tasks-permissions. Hence from the results, it is evident that DFGACT could nearly improve the security by minimizing the resources for computation.

Fig. 5 represents the rate of successful transaction with respect to time, here the DFGACT scheme has higher success rate than that of Mehraj [30]. The dynamic nature of user leads to increase or decrease of RST. Rather than the time factor, the person's conduct is considered for changes at the side of the variant of behavior functions.

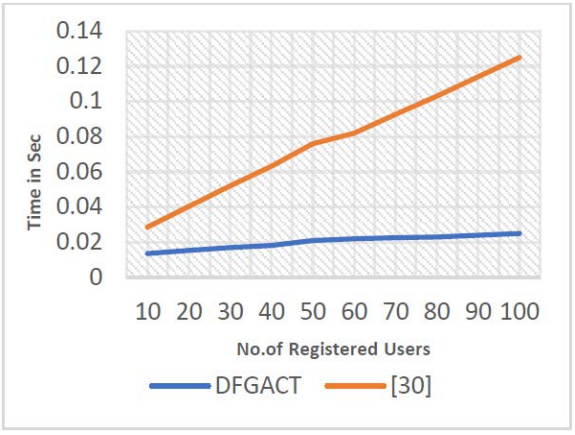

Fig. 3. Time Cost of the Schemes.

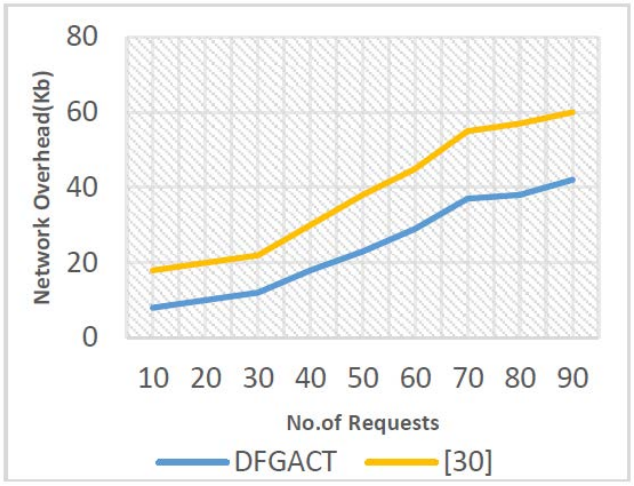

Fig. 4. Network Overhead vs. No. of Requests.

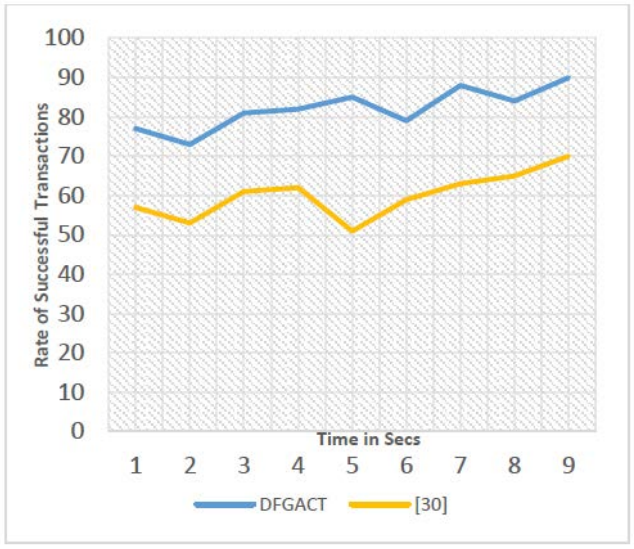

Fig. 5. Rate of Successful Transactions vs Time.

V. Conclusion

In order to reduce the computational overhead due to complex equations in encryption and decryption schemes, the distributed fine-grained access control using trust assessment has been proposed. To enable cost saving, such as time cost, network overhead and rate of successful transactions the DFGACT scheme assists in creation of multiple distribution centers for providing services to the authorized users on the basis of their trust values. To achieve fine-grained access a set of access rights list is generated for each file/resource and stored in distribution centers. The evaluations had shown that this approach has 25% more better rate of successful transactions with less time and overhead than the existing ones. In future, the application of Swarm intelligence technique for the DFGACT scheme will be implemented for handling of attacks and better throughput.

References

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng (2014) "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" : IEEE Transactions on Information Forensics and Security, Vol. 7, NO.2, April.

[2] Ravi Sandhu, David Ferraiolo and Richard Kuhn (2000) "The NIST Model For Role Based access Control: Toward a Unified Standard" : ACM workshop on Role-based access control. Vol. 2000.

[3] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang , and R. Buyya (2017), "Attributebased data access control in mobile cloud computing: Taxonomy and open issue s," Future Gener. Comput. Syst., vol. 72, pp. 273-287.

[4] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou (2013) ``Fine-grained access control system based on outsourced attribute-based encryption," in Proc. Eur. Symp. Res. Comput. Secur., Egham, U.K.: Springer, 2013, pp. 592_609.

[5] K. Yang and X. Jia (2014), ``Expressive, ef_cient, and revocable data access control for multi-authority cloud storage," IEEE Trans. Parallel Distrib.Syst., vol. 25, no. 7, pp. 1735_1744.

[6] M. Chase and S. S. M. Chow (2009), ``Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th ACM Conf. Comput. Commun. Secur. - CCS, 2009, pp. 121_130.

[7] S. Fugkeaw and H. Sato (2015), ``An extended CP-ABE based access control model for data outsourced in the cloud," in Proc. IEEE 39th Annu. Comput. Softw. Appl. Conf., Jul. 2015, pp. 73_78.

[8] Agrawal, N., Tapaswi, S. (2019): A trustworthy agent-based encrypted access control method for mobile Cloud computing environment. Pervasive Mob. Comput. 52, 13–28. https://doi.org/10.1016/j.pmcj.2018.11.003.

[9] Li, X., Zhou, F., Yang, X (2011).: A multi-dimensional trust evaluation model for large-scale P2P computing. J. Parallel Distrib. Comput.71(6), 837–847. https://doi.org/10.1016/j.jpdc.2011.01.007.

[10] G. Lin, D. Wang, Y. Bie and M. Lei (2014), "MTBAC: A mutual trust-based access control model in Cloud computing," in China Communications, vol. 11, no. 4, pp. 154-162, April 2014, doi: 10.1109/CC.2014.6827577.

[11] Khilar, P., Chaudhari, V., Swain, R (2019).: Trust-based access control in Cloud computing using machine learning. In: Das, H., Barik, R., Dubey, H., Roy, D. (eds) Cloud Computing for Geospatial Big Data Analytics, vol 49, pp. 55–79. Springer (2019). https://doi.org/https://doi.org/10.1007/978-3-030-03359-0_3.

[12] M. Rafiqul Islam and M. Habiba (2012), "Collaborative swarm intelligence based Trusted Computing," 2012 International Conference on Informatics, Electronics & Vision (ICIEV), 2012, pp. 1-6, doi: 10.1109/ICIEV.2012.6317341.

[13] V. Goyal, O. Pandey, A. Sahai, and B.Waters (2006), ``Attribute-based encryption for _ne-grained access control of encrypted data," in Proc. 13th ACMConf. Comput. Commun. Secur., Alexandria, VA, USA, 2006, pp. 89_98.

[14] J. Bethencourt, A. Sahai, and B. Waters (2007), "C iphertext-Policy AttributeBased Encryption," in 2007 IEEE Symposium on Security and Privacy(SP '07), Berkeley, France, 2007.

[15] S. Wang, H. Wang, J. Li, H. Wang, J. Chaudhry, M. Alazab, and H. Song (2020),``A fast CP-ABE system for cyber-physical security and privacy in mobile healthcare network," IEEE Trans. Ind. Appl., vol. 56, no. 4, pp. 4467_4477,Jul./Aug. 2020.

[16] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo (2014), ``An ef_cient cloud-based revocable identity-based proxy re-encryption scheme for publicclouds data sharing," in Proc. Eur. Symp. Res. Comput. Secur. (EROSICS),Wroclaw, Poland, 2014, pp. 257_272.

[17] Ye, J., Xu, Z., Ding, Y.(2016): "Secure outsourcing of modular exponentiations in cloud and cluster computing. Clust. Comput. "19(2),811–820 (2016).

[18] L. Zhou, V. Varadharajan, and M. Hitchens (2013), ``Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947_1960, Dec. 2013.

[19] Qi Han, Kan Yang, Kan Zheng, Hui Li, Xuemin Shen, Zhou Su, (2017) "An Efficient and Fine-Grained Big Data Access Control Scheme With Privacy-Preserving Policy", IEEE Internet of Things Journal, Volume:4, Issue:2, 2017.

[20] S. Fugkeaw (2019), "A Fine-Grained and Lightweight Data Access Control Model for Mobile Cloud Computing," in *IEEE Access*, vol. 9, pp. 836-848, 2021, doi: 10.1109/ACCESS.2020.3046869.

[21] He, H., Zheng, Lh., Li, P. et al. An efficient attribute-based hierarchical data access control scheme in cloud computing. Hum. Cent. Comput. Inf. Sci. 10, 49 (2020). https://doi.org/10.1186/s13673-020-00255-5.

[22] Anilkumar, C., Subramanian, S. A novel predicate based access control scheme for cloud environment using open stack swift storage. Peer-to-Peer Netw. Appl. 14, 2372–2384 (2021). https://doi.org/10.1007/s12083-020-00961-.

[23] Q. Zhang, S. Wang, D. Zhang, J. Wang and Y. Zhang, "Time and Attribute Based Dual Access Control and Data Integrity Verifiable Scheme in Cloud Computing Applications," in *IEEE Access*, vol. 7, pp. 137594-137607, 2019, doi: 10.1109/ACCESS.2019.2942649.

[24] He, H., Zhang, J., Gu, J. et al. A fine-grained and lightweight data access control scheme for WSN-integrated cloud computing. Cluster Comput 20, 1457–1472 (2017). https://doi.org/10.1007/s10586-017-0863-y.

[25] Han, Kan Yang, Kan Zheng, Hui Li, Xuemin Shen and Zhou Su, (2016) "An Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy", IEEE Internet of Things Journal, 2016.

[26] Yinglong Zhang, Shangping Wang, Yaling Zhang (2016), "A Blockchain-Based Framework for Data Sharing with Fine-grained Access Control in Decentralized Storage Systems", , IEEE Access, Vol 4, 2016.

[27] Li, Q., Zhu, H., Xiong, J. et al. (2019)Fine-grained multi-authority access control in IoT-enabled mHealth. Ann. Telecommun. 74, 389–400. https://doi.org/10.1007/s12243-018-00702-6.

[28] X. Wang, L. Wang, Y. Li and K. Gai (2018), "Privacy-Aware Efficient Fine-Grained Data Access Control in Internet of Medical Things Based Fog Computing," in *IEEE Access*, vol. 6, pp. 47657-47665, 2018, doi: 10.1109/ACCESS.2018.2856896.

[29] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay and J. J. P. C. Rodrigues (2019), "Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications," in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 457-468, Jan. 2019, doi: 10.1109/TII.2018.2824815.

[30] Mehraj, Saima & Banday, M. Tariq. (2021). A flexible fine-grained dynamic access control approach for cloud computing environment. Cluster Computing. 24. 1-22. 10.1007/s10586-020-03196-x.

[31] Mehar, Deepak & Vishwakarma, Gagan & Jain, Yogendra. (2015). Modified Fine-grained Data Access Control Algorithms for File Storage Cloud. International Journal of Computer Applications. 116. 15-19. 10.5120/20467-2288.

[32] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. F. De Rose, and R. Buyya (2010), ``CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," Softw.,Pract. Exper., vol. 41, no. 1, pp. 23_50, Aug. 2010, doi: 10.1002/spe.995.

AUTHORS' PROFILE

Ms. Aparna Manikonda worked in various prestigious institutions across India. Currently, she is pursuing Doctorate degree in computer science. She is having 15 years of teaching experience along with research and published various numerous publications. She has 8 International journal publications. She has presented papers in 15 International conferences and attended 12 Seminars/Workshops/FDP/QIP. She has organized 2 conferences, 4 workshops. She has published 2 patents and 4 books titled 'Internet and web Technology', 'Internet and Web Technology 2.0', 'Cloud computing for Beginners', 'Object Modelling using UML A software Perspective'. Her research areas include Cloud Computing, Ad-hoc and Sensor networks, IoT and Image Processing.

Dr. N. Nalini is a Professor in the Department of Computer Science and Engineering at Nitte Meenakshi Institute of Technology, Bangalore. She received her MS from BITS, Pilani in 1999 and PhD from Visvesvaraya Technological University in 2007. She has more than 24 years of teaching and 17 years of research experience. She has numerous international journal and conference publications to her credit, She has served as Technical Committee member and reviewer in various International conferences and has delivered technical talks at various Institutions. She Published book on "INTERNET OF THINGS: Advanced Wireless Technologies for Smart Ecosystems" having ISBN-13: 979-8679630055. Recognized as FSIESRP (Educational- Professional Membership Grade: Fellowship) & Editorial Board Member Registration as Hon. Consulting Editor. Program Committee Member in BIOMA International Conference since 2010. Organizing Committee Member in the Congress of the "International Conference on Electronics & Electrical Engineering" Seoul, South Korea. She has guided EIGHT candidates to complete their Ph.D successfully and currently guiding five more candidates. She has guided more than fifty PG students to complete their thesis. Her areas of research include Cryptography and Network Security, Cloud Computing, Artificial Intelligence and Machine Learning, Wireless and Distributed Sensor Networks, Optimization Heuristic Techniques.