iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** X **Month of publication:** October 2018

DOI:

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

An Improved Cloud Security Model by Attribute-based Access Control using Enhanced Bell-Lapadula Model in Cloud Computing

Miss Nidhi Saxena
Gautam Buddha university, Greater Noida, Yamuna Expressway ,Indi

Abstract: ***Cloud computing is one of the emerging technologies that is being used widely these days. It makes use of the computing resources such as hardware and software that is delivered over the internet and provides remote services with user's data, software and computation. There has been a growing trend to use the cloud for large-scale data storage. This has raised the important security issue of how to control and prevent unauthorized access to data stored in the cloud. There are various access control techniques in cloud environment such as IBAC, RBAC, ABAC, MAC, DAC. Among these techniques, Attribute-Based Access Control (ABAC) is gaining more importance. Here access is granted based on attributes. Our primary objective is to summarize all the access control techniques in cloud environment. Our main objective is to come up with a Novel Attribute-Based Access Control for cloud security using Enhanced Bell-Lapadula Model inspired from Honey Bee behaviour.The Honey Bee prevents the intruders from entering into their hives. This is similar to the access control mechanism in cloud environment. It identifies the bee that belongs to the same hive by the possession of the small barbs on the stings. Similarly, we are trying to restrict the users based on the possession of correct set of attributes by using ABAC technique.***

Keywords: Attribute Based Access Control, Bell-Lapadula Model, Cloud security, Role based acess controls

I. INTRODUCTION

In this era of information technology, the users could enjoy more advantages in terms of internet and network facilities. On the whole, it seems to be more beneficial and useful but there is also a bitter side of it in terms of providing and preserving an individual's privacy in a highly distributed environment where the number of users keeps increasing. In this scenario, it is highly recommended to preserve the shared data and contents to assure the privacy of each and every user in the system. This gives rise to the need for a term called "cloud computing". Cloud computing is about using the services that has been deployed in the cloud by the third parties from remote locations wherever the network facilities are available[1]. Users enjoy freedom in using the cloud services by "Pay as You Use" so they can decide their usage of the network resources. For instance, social networking websites, e-commerce applications and many of the major enterprises use and depend upon the shared resources from cloud. There is a terminology called "ACCESS CONTROL" used in cloud environment. It deals with determining who can access, read and modify the data deployed in cloud [2] .It allows access to those users who has the accurate access permissions and possess certain identities in terms of roles and attributes. Also, it restricts the access to unauthorized persons to ensure the security and confidentiality. Although many access control models prove to be beneficial and confidential, the privacy preservation in the distributed environment has not been solved yet. Traditional models like DAC, MAC and RBAC proves to be obsolete in meeting the needs of the End users. To begin with, the DAC(Discretionary Access Control)model uses the concept called Access Control List(ACL)[4].Instead of using the AC matrix ,which does not provide high level security, it is highly desirable to use this type of mechanism. The ACL will describe who can access what resources based on the ownership of the resource. In addition, it lists the objects and the authorized subjects who possess the right access to process it. It is more flexible in the distributed environment [5]. The main drawback of this is that it cannot recognize the users and computer separately while they are accessing the objects. In Label-based Access Control model, the data is modelled into rows, columns or both. The user who wants to access the data will be provided with labels. Those users who possess correct labels will only be provided access and others will be restricted to proceed with thereby ensuring the security of the data. The labels like system administrator, manager, CEO could be granted or revoked based on the access permissions. Initially, the model called Mandatory Access Control (MAC) [6] is formed by making use of the label-based user restrictions from accessing the confidential files. This model is purely under the control of system administrator and user has no job in defining and modifying the access control policies for resources. The system administrator will configure the operating system's default setting that controls the resource permissions. All the resources in the cloud will be assigned security

labels which are split into two, namely classification and category. Similarly, the subjects are provided with security labels before they request a permission to access a particular resource. When any user tries to access a resource, the operating system first checks out the matching of the security labels of both user and the resource. When both the security labels (i.e. classification and category) match perfectly, the user will be granted access/permission to proceed with his/her desired resource usage. Else the user will be restricted to proceed further and his access permission is denied. Thus MAC proves to be more convenient and beneficial in granting secure environment for cloud users thus spreading its importance in highly confidential military applications. On the contrary, it has some disadvantages. To list few, considerable amount of time must be devoted in planning the access decisions before actually they come into picture. The management and updating process of user and resource security labels proves to be a tiresome job.

Instead of permitting the access policies based on labels, there is an alternative approach which gained more importance in cloud security. It is about providing access rights based on the roles possessed by the user in an organization environment. It is formulated by combining the concepts of DAC and MAC. Basically, the function/role-based access control method has two mappings [7]. One is from user to roles and another is from roles to privileges. There are 3 rules based on which the RBAC scheme operates. They are Role assignment, Role authorization and Permission Authorization. These roles have hierarchical structure and the access is given to the users based on the user's roles rather than based on the user themselves. So, even when the roles are removed or revoked, it is not mandatory to change the access permissions that has assigned to that roles. This scheme overcomes the disadvantages of the previous models and it is more flexible paving way for many enterprises and organizations to formulate their access policies without violating their organization structure and policies. But the main drawback is that since the access is based on user's roles rather than the user himself, it is difficult to retain and reallocate the roles and permissions for users after change of their positions and job titles in the organization hierarchy. So it is highly recommended to develop a new access control based on attributes of the user so that the user could enjoy the cloud usage and simultaneously protecting his privacy data and information.

II. RELATED WORK

Due to the various limitations encountered in RBAC schemes, steps have been taken by the researchers to focus on user's attributes rather than focusing on user's roles. The reason behind this is maintaining the user's roles and managing the access permissions in an organization hierarchy proved to be a tiresome job and leads to management overhead. Also, retaining the role-permission stability is complex when the particular user has been revoked from his position. Hence to resolve these complexities, the concern is given towards Attributed based access control[8]. ABAC's working mainly directed towards analysing the user's attributes and thereby restricting the unauthorized users and malicious intruders. These attributes maybe of three types called Subject attributes, Resource attributes and Environment attributes. The subject is actually the user who is accessing the resource from the cloud. The subject attributes include the user's ID, name, job title, DOB, gender, national number, etc. The resources are the objects that are used upon the subject. Each resource possesses unique attributes in terms of file name, file size, file access mode, etc. The environment attributes includes information about where the access takes place, i.e. the place or surrounding.

In [9],Attribute-Based Access Control is gaining more importance in today's cloud environment due to its flexible and scalable nature. But its internal issues remain still unresolved. One among them is the lack of reference model to describe about the non-trivial security properties. In this paper, they have proposed a mapping between the attributes and access policies by introducing the concept of "security tokens".Though this system provides a reference model, it lacks the actual prototype for the non-realistic experiments.

In [10], real-time applications, there are time constraints to access the resources present in the cloud. Current access control models such as RBAC and ABAC do not provide real-time extension in a scalable and flexible way. To resolve this, they have proposed a new enhancement of ABAC called real-Time-ABAC (T-ABAC) in this paper. T-ABAC involves the use of real-time attributes and prioritizes the access requests from the user based on these attributes. The only disadvantage is that the strict time constraints, which lacks the user-friendliness in the distributed environment where multiple users share resources simultaneously.

In [11], the behavior of honeybee colonization provides a source of inspiration to enhance the currently used cloud environment. The Honey Bee prevents the intruders from entering into their hive. This is similar to the access control mechanism in cloud environment. In this paper, they have proposed a load balancing algorithm inspired by honey bees foraging behavior. This paper works only for independent factors and no extension for in QoS parameters.

In [12], this paper, the access control policies are enforced for an education cloud. The sharing of information among the schools involves many challenges including technical issues like copyrights and social issues like cooperation between the teachers and parents. So, it is highly desirable to provide an efficient access control model for this type of scenario. ABAC resolves these issues

by authorizing the student based attributes like student's grade, electives, assignment etc., and it proves to be efficient by using Class-Algebra which formulates the users, roles, and services. But, this works well only in case of centralized systems but not in decentralized (distributed) systems.

In [13], nowadays, many organizations use a combination of internal (private) cloud along with the public cloud. But this raises the issue of dividing the applications along the cloud. Presently this has been resolved by using ad-hoc approaches. Ad-hoc approach proves to be error-prone and avoiding many benefits. In this paper, they are implementing one of the Multi-level Security model called Bell-Lapadula Model to encounter the various issues in cloud computing. The BLP model sees only data confidentiality and ignores data integrity.

III. PROPOSED ALGORITHM

A. Attribute Based Access Control

Almost all the present system environment runs based on the Role Based Access Control (RBAC) model where users are identified by their roles. There are two mappings in this system. First, the user is assigned to roles, and then the roles are assigned to permissions. These permissions include read/restricted write/write permissions to access the protected resources. But the main drawback is that since the access is based on user's roles rather than the user himself, it is difficult to retain and reallocate the roles and permissions for users after change of their positions and job titles in the organization hierarchy. Due to the various limitations encountered in RBAC schemes, steps have been taken by the researchers to focus on user's attributes rather than on user's roles. The reason behind this is maintaining the user's roles and managing the access permissions in an organization hierarchy proved to be a tiresome job and leads to management overhead. Also, retaining the role-permission stability is complex when the particular user has been revoked from his position. Hence to resolve these complexities, the concern is given towards attributed based access control (ABAC). Hence, it motivated us to combine the ABAC techniques with the BLP model to provide more security in terms of access permissions and usage.

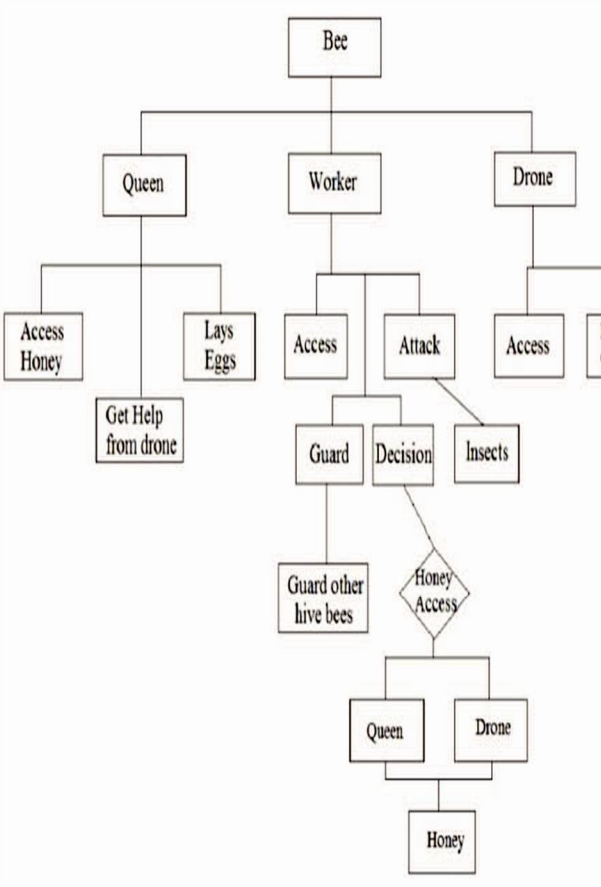


Fig 1. Honey Bee Hierarchy

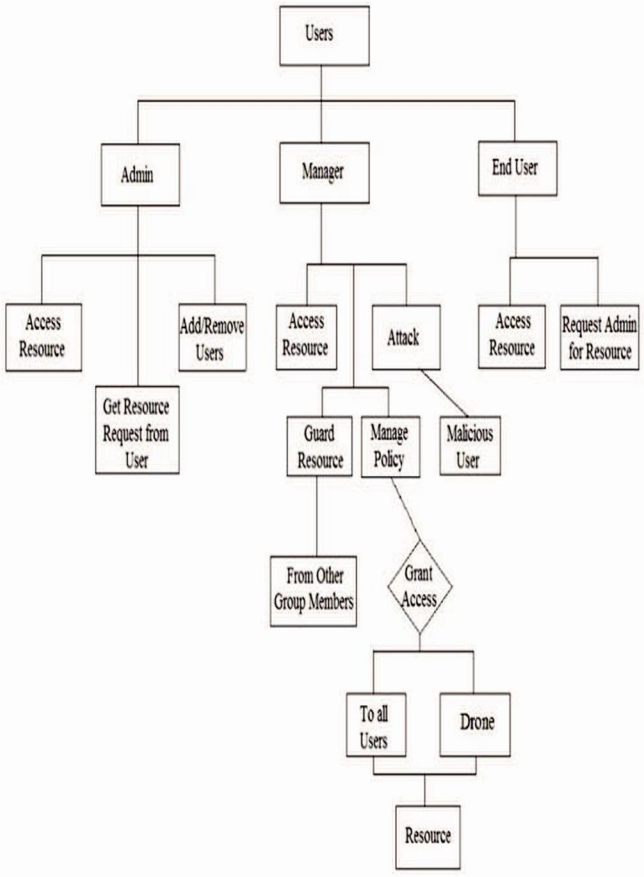


Fig 2. Access Control Hierarchy

B. Inspiration From Honey Bee Behaviour

Honey bees possess different character in identifying the intruders which belongs to other hives from attacking their hives and steal honey from it. The worker bees look for the possession of the small barbs on the sting of the each bee. It restricts the other bees (intruders) which try to gain access to the hive illegally. The worker bees owns and maintains the hive and provides a higher level of security for the Queen bee and Drone bees[11] .This behaviour of honey bee provides a source of information to enhance the present problems in cloud environment. The confidential users could be identified by the correct set of attributes which is similar to the possession of the barbs in the worker bees. This inspiration has driven us to enhance the existing problems in ABAC technique.

C. Bell-Lapadula Model

Initially Bell-Lapadula model [14] use role of users and objects as matrices to provide access. Based on security label of user, the access of particular object by the user is determined. Now the attributes of the users are embedded in matrices of Bell-Lapadula model. To increase the security level cipher encryption is added to each of the attributes based on the master security key and public key. By fixing the encrypted attributes in the matrices of the Bell-Lapadula model it provides an extra security for access. When dealing with Bell-Lapadula model, it is mainly used to solve the confidential problem of access control paradigm. It can effectively prevent the information to flow from higher security level to lower one. Also, the existing Bell-Lapadula model makes use of the user's roles and assigns keys based on it. The access "Read" is provided when the security label of the subject is less than the security level of the object. On the contrary, the access "Write" is provided when the security label of the subject is higher than the security level of the object.

D. Bell-Lapadula Policy Read/Write Policy

1) Get the user attributes.
2) Checks the access matrix with the keys and roles of user to provide the read/write access to user
3) If the security label (subject) < security level (object) Access=Read.
4) If the security label (subject) > security label (object) Access=write.

E. In General,

Bell-Lapadula model checks with user roles and keys Ex. 1.Sujects are say (x, y) who can be staff, admin or developer
2. Objects are (p, q)
But the main drawback is that since the access is based on user's roles rather than the user himself, it is difficult to retain and reallocate the roles and permissions for users after change of their positions and job titles in the organization hierarchy. It mainly deals with Data Confidentiality rather than Data Integrity. Also covert channel is present in this model, but not addressed comprehensively. Covert channel is nothing but an information channel. There is no specific strategy to modify the access control authorities and classification levels. So, it is highly desirable to enhance the BLP model such that it meets the changing security requirements along with using the attributes of the user in identification modules.

F. Our Algorithm

Due to the various limitations encountered in RBAC schemes, steps have been taken by the researchers to focus on user's attributes rather than on user's roles. The reason behind this is maintaining the user's roles and managing the access permissions in an organization hierarchy proved to be a tiresome job and leads to management overhead. Also, retaining the role-permission stability is complex when the particular user has been revoked from his position. Hence to resolve these complexities, the concern is given towards attributed based access control (ABAC). Hence, it motivated us to combine the ABAC techniques with the BLP model to provide more security in terms of access permissions and usage. Our proposed system consists of enhanced BLP model along with ABAC inspired from Honey Bee Behavior.An enhancement in terms of integrity levels helps to resolve the current limitations of BLP model. So, instead of defining each subject (user) at security level, both subjects and objects can be defined at integrity level. Henceforth, it brings new changes in the BLP model to meet the changing security requirements. The Behavior of honeybee colonization provides a source of inspiration to enhance the currently used cloud environment. The Honey Bee prevents the intruders from entering into their hives. This is similar to the access control mechanism in cloud environment. It identifies the bee that belongs to the same hive by the possession of the small barbs on the stings. Similarly, we are trying to restrict the users based on the possession of correct set of attributes by using ABACs technique. Hence, in the enhanced BLP model, attributes) to ensure the privacy of the users. the read/write access is given based on both (roles +

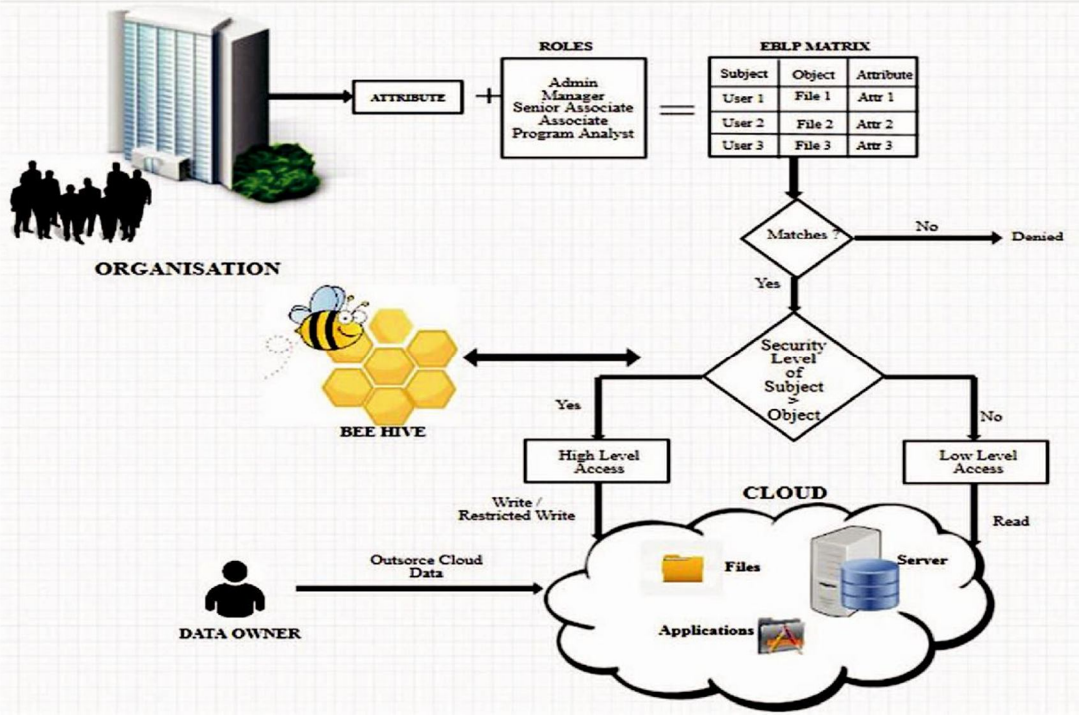


Fig 3. Architecture Diagram

G. Enhanced Bell-Lapadula Policy

1) Read/Write Policy

a) Get the user attributes.

b) Associates the roles and attributes with the keys in the access matrix.

c) If the security label of the subject (Role + Attribute) < security level (object) Access=Read.

d) If the security label of the subject (Role + Attribute) > security level (object) Access=Write.

2) An Enhanced Bell-Lapadula contains

For Ex:

a) Sujects are say (x, y) who can be staff, admin or developer

b) Objects are (p, q)

c) Attributes include the qualification, location etc. Normally in a bee hive, the unauthorized bees from a different species are restricted from entering into the hive by following the following mechanism:

{B +b } Honey Access

Here 'B' implies the possession of small organ called 'Barbs' on the sting of the Honey bee.
And 'b' implies the role of the Honey bee which could range from Queen, Drone and Workers.
This environment could be related with the cloud scenario where the users with the correct set of attributes and roles will be availed with access permissions to the particular resource in an organization. Mathematically it could be stated as,

{A+R} Resource Access

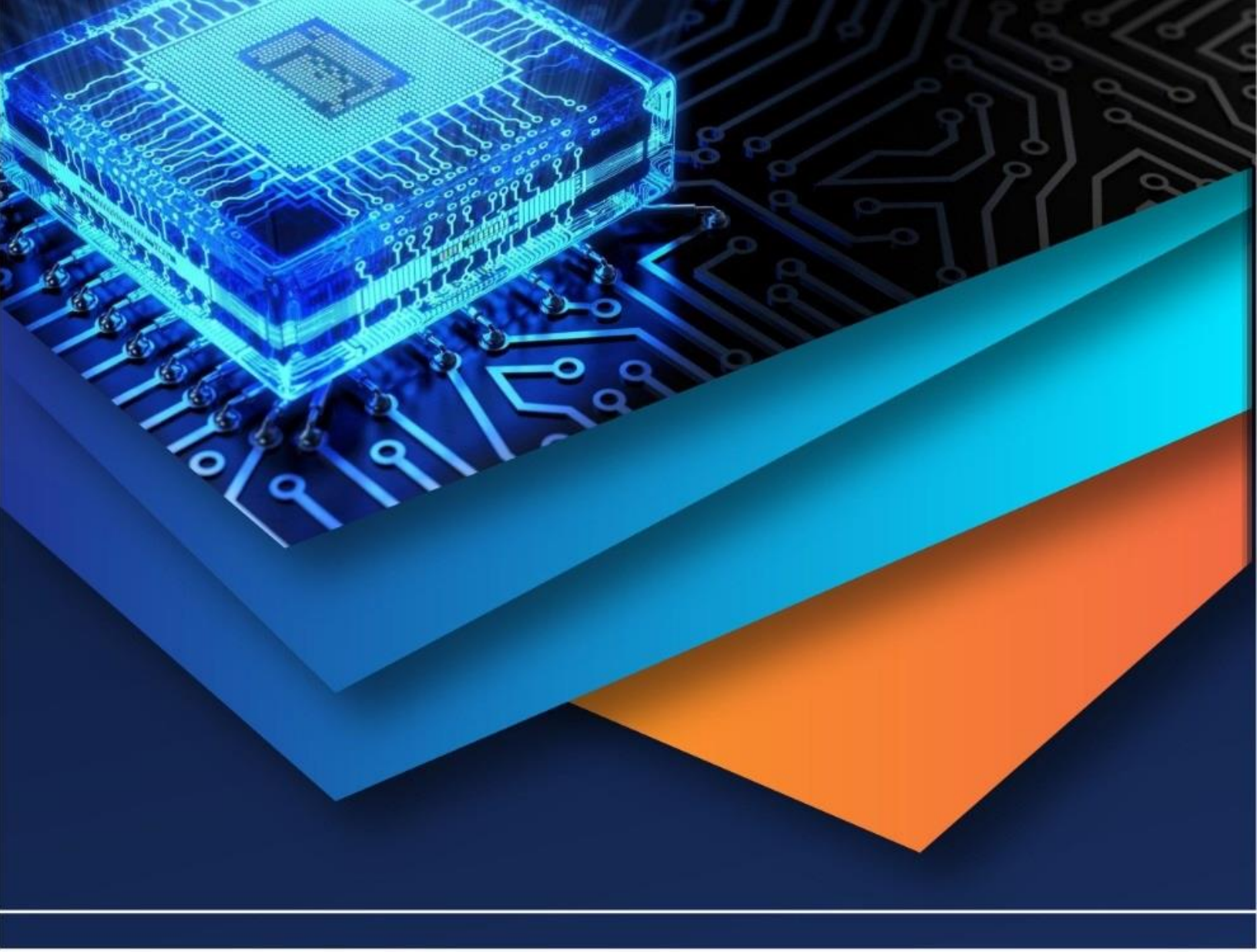
Here, 'A' stands for Attributes of the user such as the Name, Age, Gender, Group-id, Group-name
And 'R' stands for the Roles of the users such as Administrator, Manager, Developer.
Consider in an organization, a new group of users say Group A is formed for completing a new project say Project A. To provide high level access to the members of the Group A, the attribute of the group called 'A' could be combined with the individual roles of the members of the Group.

IV. CONCLUSION

Due to technology advancements, it has become simple and easy to hack other's private information in a network. Thus it arises the need for Access Control in Cloud Computing and in our system, we used Attribute Based Encryption (ABE) along with enhanced BLP model inspired from the behavior of Honey Bee, to ensure privacy and make the users feel secure to store and retrieve the data to and from the cloud. So it is highly recommended to encrypt the most sensitive information before deploying them in the cloud. The data owner alone owns the respective decryption keys and they outsource the data only to the authorized users based on their attributes. When the attributes match, the resultant user is provided with the corresponding keys to access and use the sensitive data. Our System proves to be more beneficial for adding new users with lower level access policies. So that they can be added to a higher-degree group to access the higher-level information. In addition, the users could be relieved from the group if they no longer needed to maintain the privacy of the higher-level information. This flexibility makes the cloud computing paradigm more secure and efficient.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, Tech. Rep., 2009.
[2] Haibo Chen, Fan Hong, "Survey of Research on Access Control Model," Application Research of Computers, vol. 6, Mar. 2005, pp. 9-11, doi: CNKI:SUN:JSYJ.0.2005-06-003.
[3] B. W. Lampson, "Protection ACM SIGOPS Operating System Review", 8(1):18–24, January 1974.
[4] Mark S. Miller, Ka-Ping Yee, Jonathan Shapiro, "Capability Myths Demolished", Technical Report SRL2003-02, Systems Research Laboratory, Department of Computer Science, Johns Hopkins University, March 2003.
[5] Bishop, Matt, "Computer security: art and science", Addison-Wesley.ISBN 0-201-44099-7, 2004.
[6] Zhang Lei, Zhang Hongli, Yin Lihua, Shen Xiajiong, "A Mandatory Access Control Model Based on Concept Lattice", 2011.
[7] D. Ferraiolo and R. Kuhn, "Role-based access control", 15th National Computer Security Conference, pages 554–563, October 1992.
[8] V.Goyal, O.Pandey, A.Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings ofthe 13th ACM Conference on Computer and Communications Security(CCS'06). ACM, 2006, pp. 89–98.
[9] Carlos E. Rubio-Medrano, Clinton D'Souza and Gail-JoonAhn, "Supporting Secure Collaborations with Attribute-based Access Control", IEEE, 2013.
[10] Mike Burmester, Emmanouil Magkos and Vassilis Chrissikopoulos, "T-ABAC: An Attribute-Based Access Control Model forReal-Time Availability in Highly Dynamic Systems", IEEE, 2013.
[11] Dhinesh Babu L.D., P. Venkata Krishna, "Honey bee behavior inspired load balancing of tasks in cloudcomputing environments", Applied Soft Computing 13, 2013.
[12] Daniel J. Buehrer, Chun-Yao Wang, "CA-ABAC: Class Algebra Attribute-Based Access Control" IEEE, 2012
[13] Paul Watson, "A multi-level security model for partitioningworkflows over federated clouds", Watson Journal of Cloud Computing: Advances, Systems and Applications, 2012.
[14] Jin Jing, ShenMeihui, "Analysis of Security Models Based on Multilevel Security Policy", IEEE, 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY