Multilevel Cloud Security Policy (MCSP) for Cloud-Based Environments

Priya Oberoi, Sumit Mittal, Rajneesh Kumar Gujral

Abstract: In the present period Cloud computing(CC) generally addresses the issues of quick arrangement and on-request versatility. Despite the fact that Cloud computing gives countless benefits to the clients like adaptability, versatility and so on however, it additionally brings new security challenges.

In this paper, authors have proposed a Multilevel Cloud Security Policy (MCSP) to provide security in Cloud-based environment from the malicious insider attacks. This policy comprises of two levels viz. Cloud Chinese Wall Security Policy (CCWSP), and Cloud Clark Wilson Policy (CCWP).

At the outer level of MCSP, CCWSPoperates, whileat the inner level operates CCWP.Whenever a client endeavors to access services provided by the Cloudor administrations then its demand is either allowed or dismissed by the CCWSP.Now, if the client gains admittance to the asked for administration or services,then within that service or domain the authorization is done using the CCWP. The MCSP is proposed to mitigate the malicious insider attacks at IaaS in Cloud-based environments. Being a multi-level policy it is capable to detect as well as prevent the malicious insiders within the tenants of the clouds as well as within the organizations.

Keywords:Cloud Security, Malicious Insider Attacks, ChineseWall Policy, Clark Wilson Model.

I. INTRODUCTION

The present era is era ofmodern computing. Every aspect of human life is witnessing a drastic change. Whether it is business, movies, games, cooking or education, the day to day life of the whole world is depended on the Internet. Social media has become a necessity of life. Everybody is readily sharing personal photos, data, and bank information on websites. A huge amount of data is being stored and accessed on the Internet. Thus, to deal with this data researcher and pioneers concocted the idea of the Cloud[1][2][3].

But still, the Clouds have not been recognized as a secure media as it involves the transfer of critical information through the public Internet.The integrity and confidentiality of the user’s data are at risk as they do not have physical control over the data[4].The Cloud computing platform has heavy leads and frequent accesses from an oversized variety of users that requires various dimensions of security[2][5].

The most important aspects of security are confidentiality, integrity, and availability(CIA). These can be accomplished by keeping up the agreementbetween generally accepted security models;those in turn can be accomplished by implementing the latest security techniques, risk management methods, and sound management principles.Cloud computing is vulnerable to a number of attacks such as Data breaches, Advance Persistent Threats(APTs), and Denial of Service(DoS)[6]. Today malicious insider attacks have become part of the real world and destructive results can beclearly identified[7]. The effect of insider attacks is more severe in Cloud-based environments than in traditional environments. Hence the insider threat is critically challenging in the Cloud-Based environments[4]. Security is required from attacks as well as from malicious use of the data.

In Cloud-based environments, the compromised Virtual machines or devices can gain access to the services offered by the Cloud in a normal manner. These devices use a valid identity to perform the attack[8].

The malicious insider can also be an authorized person with all the administrative powers and rights. This insider can knowingly or unknowingly use its access rights in a malicious way to harm the system. The main aim of malicious insider can be to snip the information of the organization and deliver it to the competitors[9][10].

So to detect and prevent this kind of activity of a malicious insider a Multilevel Cloud Security Policy (MCSP) has been proposed. As in case of public Clouds, there are multiple tenants; there is a possibility that the competitors can gain access to the data of rivals. This access can either be intentional or unintentional. The proposed security policy in this paper is capable to detect both of these. Being a multi-level policy it is capable to detect as well as prevent the malicious insiders within the tenants of the clouds as well as within the organizations. This exceptional feature of MCSP makes it adaptability easier in the real world.

The users of the Cloud computing environment are very much prone to internal attacks. In order to eliminate the possibility of internal attacks, in general, and malicious insider attacks, in particular; Multilevel Cloud Security Policy (MCSP) has been proposed in this paper. The authors have built the

Revised Manuscript Received on May 22, 2019.

PriyaOberoi,M.M. Institute of Computer Technology & Business Management, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India.

DAV Centenary College, Faridabad, Haryana, India

Dr. Sumit Mittal, M.M. Institute of Computer Technology & Business Management, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India.

Dr. Rajneesh Gujral,M.M. Engineering College, Maharishi Markandeshwar(Deemed to be University),Mullana,Ambala, Haryana, India.

security policy to increase the security level in Clouds.Cloud computing is a combination of hardware, software and storage capacity which are provided as IaaS, SaaS, and PaaS. The workin this paper mainly focuses onIaaS.

II. CHINESE WALL MODEL

Chinese wall model is a very popular model used by the organizations. This model addresses the two important aspects of the security i.e. privacy and data integrity.This model uses Mandatory access control (MAC) and Discretionary access control (DAC) collectively, which are the key components of access control[5][11][13].

The key concept of this model is to break the entities into a group of classes. A user with the access privileges has access to information only to its own class and all the other classes which are not of its domain or business area.This helps to prevent the conflict of interest which may arise when for competing activities a single person is responsible. Data is classified into sanitized and un-sanitized zones.Brewer-Nash proposed two rules as an enforcement mechanism[14].

The first is a simple security rule and the other is ∗-rule. These rules are the necessary conditions which a system is expected to follow before granting access to a subject[15].

Simple security rule: Subject S can have read access to object O only when:

1. There's associate object O´ specified S has accessed O´ and CD(O´) = CD(O).
2. For all objects O´, O´ ∈ PR(S) ⇒COI(O´) ≠ COI(O).
3. Sanitized object is O.

where CD refers to company dataset and COI refers to Conflict of class.

CW-*- Property: Asubject S could write to associate object O, if and provided that each of the subsequent conditionshold:

1. Subject S reads object O according to simple security rule.
2. O’can be read by S O´ ⇒ CD(O´) = CD(O), where O’ is a unsanitized object.

Chinese wall policy finds its applicability into many fields as it gives the features of mandatory enforcement and independent choice of users. There are different access control models which are proposed based on Chinese wall policy and can be enforced within the Cloud effectively[16].

III. CLARK- WILSON MODEL

The primary goals of integrity protection are[13][17][18]

1. Prevention from modification by an unauthorized user.
2. Data consistency maintenance, and
3. Prevention of authorized user to alter the data in unauthorized ways.

Clark Wilson model is the only model which achieves all these three goals. This model doesn’t allow direct access and control to the objects.

CW model divides the data of the system in two categories[19]

A. Constrained data items (CDIs): These are the items which are already part of the system and need the integrity to be maintained.
B. Unconstrained data item (UDIs): These are the items which are recently brought into the framework and are not secured by integrity policy, but rather they have significance as they are changed over into CDIs.

CW model mainly applies a set of two procedures:

A. Integrity verification procedure (IVP):It confirms that the state of all CDIs is valid. The IVP maintains the consistency of the system.
B. Well-formed transformation procedure (TP):Transformation procedures (TPs) can control the CDIs as they change a lot of them starting with one substantial state then onto the next. Well-formed transactions are implemented by these.

TPs can only alter the data which help in maintaining integrity. If the alteration results in violation of integrity then it is not allowed. Specific integrity policy is used for certifying the IVPs and TPs. The TP must meet its details and these must be right. The latter framework must necessitate that all change methodology be recorded in the logs, giving a following and inspecting component for all changes. Figure 1 shows a well formed TP which is performing operations on two CDIs.

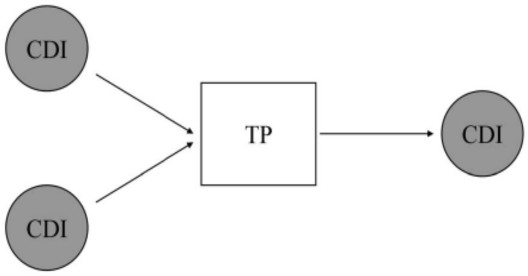

Figure 1. A well-formed TP operating on two CDIs

A set of enforcement rules and certification rules are used for the working of this model[20]. Enforcement rules specify what a system can maintain and certification rules specify what is allowed to entities which are outside the system. Separation of duty and general access control is used for restricting TP’s. It is done to control the operations of users of TP’s on particular CDIs.CW model is based on basic nine rules:

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Rules for Certification

- **C1 (Certification by IVP)** –The integrity of CDI is validated using an IVP.
- **C2 (Validity) –** The TP should be applied to a CDI in such a manner so that it maintains the integrity of the CDI. The certification of a CDI should be done to make sure that it leads to a valid constraint data item.
- **C3 –**A TP only can make alterations in CDI. The certification of TPs should be done for ensuring that the principle of least privilege and separation of duties are implemented.
- **C4 (Certification of logs)**–The actions of the TPs are appropriately logged by certifying the TPs.
- **C5 –**The certification of TPs is required in order to ensure that the action of TPs lead to a valid constraint data item.

Rules for Enforcement

- **E1 (Validity Enforcement) -** The framework must keep up a list of the relations of principle C2 and must guarantee that any control of a CDI is through a TP and is approved by some connection.
- **E2 (Enforcement of Separation of Duty) -** The framework must maintain a list of relations that unite the client, the TP, and the CDIs that the TP must control for that client.It is called access triplet (client, TP,{CDI set}).
- **E3 (User Identity)** –The system should attest the identity of every user trying to execute a TP.
- **E4 (Initiation)** –The administrator solely will specify TP authorizations

In this model, an unauthorized user cannot alter data or programs[19]. It is the access triple which prevents unauthorized access. This model ensures the integrity, access control and auditing, definedas:

- **Integrity:** Rules C1, C2, C5,E1, and E4 ensure integrity. Here integrity implies that CDIs can be altered only in a constrained way so that it produces a valid CDI.

- **Access control:**Rules C3,E2, and E3 ensure access control, which implies the capability to restrict access to resources.

- **Auditing:**Rules C1 and C4 make sure the auditing. This makes sure that the system is in an exceedingly valid state.

The CW model prevents unauthorized users from altering the data and authorized users from making an improper modification. It also maintains internal and external consistency.

IV. RELATED WORKS

Kesarwani and co-authors built model at the IaaS level of Clouds to implement separation of duties and access control. The model is based on the Chinese WallModel. In this work, the nodes of the Clouds are grouped in the form of a cluster. Every cluster is sanitized to provide the functionality of the Chinese wall model. However, the limitation of this work is that it does not cover indirect COI threats [12].

Yu et al. gave a defense mechanism for side channel attacks in Clouds. A scheme called security-awareness VMs management scheme (SVMS) is presented. A three-step process is used in this scheme. At first, user constraint relations are described using the aggressive conflict of interest relation (ACIR) and aggressive in the ally with relation. Then four isolation rules are used which are based on Chinese Wall Policy. In order to give isolation of virtual machines(VM) in the conflicting users, VM placement and migration algorithms are implemented at the third step. The major feature of this scheme is that it is free from complicated decision making and monitoring systems. Also, it assures the isolation in conflicting classes among the VMs. The limitations include the high cost of VMs migration and not capable to isolate users according to VM traces [16].

Tsai and co-authors proposed Chinese wall central management system (CWCMS), to mitigate the inter-VM attacks[21]. An internally built Cloud is used for the experiments which use a kernel-based virtual machine (KVM). This CWCMS restricts the virtual machines from deployment and migration. The authors used Trick's graph coloring algorithm for analyzing the conflict of interest relations. The proposed model has two layers viz. Chinese wall central server and virtualization platform having a Chinese wall control agenda. In this system after a VM is loaded and executed on a physical machine, no more VMs of the same COI are allowed to get executed on the same physical machine. The proposed method is better in terms of utilization of resources. Limitation of this work is that no results are shown to prove that the security mechanism is strong enough.

In the work by Ge and Polack architecture for data base management (DBMS) which uses the Clark-Wilson security has been presented[22]. The main focus of this research is on the integrity of databases and access control. According to the authors, all the integrity constraints enforce CDI integrity under access and modification by TPs. At the first step,the validation of UDIs is done using the rule C3 and C4. Secondly, the enforcement rules E3 and E4 are implemented on CDIs.

Fehis and Noualiproposed a Chinese security policy. This implementation relies on the access query type of the subject to the objects. In this model initially, a wall is created around the subject and then another wall is created around the object. Every subject has a (Grant,Denied) and object has a (Conflict,Allied) security labels. Read/write query is executed according to rule "We cannot find two complexity data inside the same wall". This model is implemented in a distributed system using the object-oriented program[23].

Alqahtani and Gamblegave the concept of centrally storing and monitoring COI classes for the services of the Cloud. A security monitoring database is built which act as

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

repository and resources for auditing the COI classes[24].

She et al.studied COI in SaaS. Their study specifically focused on issues related to information flow control issues. All the services provided by Cloud are directed to follow the information flow control rules. Every service applies its own policies to define how sensitive information will flow among the various services. The service chain should have the policies which fulfill the needs of the user. The limitation of this model is the inability to resolve the issues of COI when the level of message transfer is high[25].

Wu et al. studied the problem of information flow at the IaaS layer of the Clouds. In the given solution Chinese wall model is used. However, the solution doesn't take into account the disclosure of information due to the exchange of messages between services and data resource. It only consideredhuman users. Another limitation of the model is that it doesn't handle the violation of COIs which are indirect in the service chain. It deals only with the direct COI violation of the objects[26].

In another work by Shen et al. a solution forthe problem of data isolation in Clouds is presented. The main focus of this work is on Cloud storage. The Chinese wall model (CWM) is used to handle the conflict of interest(COI) threat among the tenants of the Clouds[27].

V. THE MULTILEVEL CLOUDSECURITY POLICY (MCSP)

In IaaS the Cloud is divided into nodes and a set of nodes form a cluster. The clients of the Clouds are mostly concerned about the availability of the data. The data should be readily available to the client. The client does not have to bother about the details that how the data is stored, how it is accessed etc.. It is the responsibility of Cloud manager to implement and maintain the segregation of duties in Clouds. For example, in an organization, the admin of the system and the accounts manager of the system have different requirements of data. So, they should be allowed to access the data according to their positions and need. It means they should be able to access only that data which is relevant to them. So,to solve this issue the authors have taken an initiative to implement the access control and segregation of duties in Clouds. This is done by using the CloudChinese Wall Security Policy and CloudClark-Wilson Policy.

The proposed model uses the “Conflicting Classes” and “Segregation of duties”. Conflicting classes are the classes which can be accessed by any user of the Cloud. The conflict classes help the manager of the Cloud to implement the access control mechanism in a better way which inturn increases the efficiency of the Cloud.

Among the various levels of Clouds, only IaaS is suitable for implementing the Chinese wall policy. This is due to the fact that IaaS offers physical infrastructure for the storage of user's data. As compared to other levels IaaS is more practical to apply the Chinese wall policy.

The authors present a security mechanism to detect and prevent malicious insiders in Cloud-based environments. According to the proposed work, at the outer-level, the CCWSP operates (Figure 2). Initially, any client is allowed to access any data of the Cloud in any dataset class. A Cloud Chinese wall is created once a client accesses a dataset class. Now, this client can no more access any dataset of the same conflict of interest class.

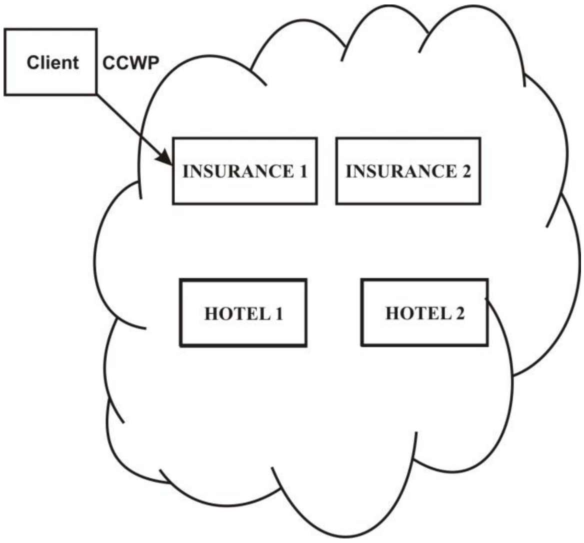

Figure 2 Position of CCWP in MCSP

Once a user gains access to any COI class then, within that COI class the CCWP operates. CCWP allows user actions which do not violate the data integrity rules. A user with valid authorization is allowed to gain access to the data. User's requests are granted or revoked according to their privileges (Figure 3).

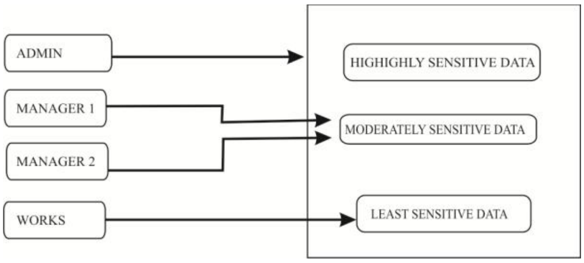

Figure 3 Privileges of users according to roles

A. *Cloud Chinese Wall Security Policy (CCWSP)*

The Chinese wall model is a commercial security policy which deals with integrity and confidentiality. This policy is used for separation of people having conflicting interests. This helps in the security of shared information.

In a cooperate network an authorized user having a conflict of interest is known as malicious insider. This individual has full authorization related to his job functions[28]. Therefore his chances to make harm to the organization are more than a regular attacker. The Cloud Chinese wall security policy(CCWSP) does not allows any internal attack to occur.

CCWSP is the policy which divides the data in into conflict of interest(COI) classes. No user is allowed tocross the boundaries of the COI classes.According to the two theorems of the Chinese wall model, any novel subject can gain access to any of the COI class at the initial stage(figure 4).

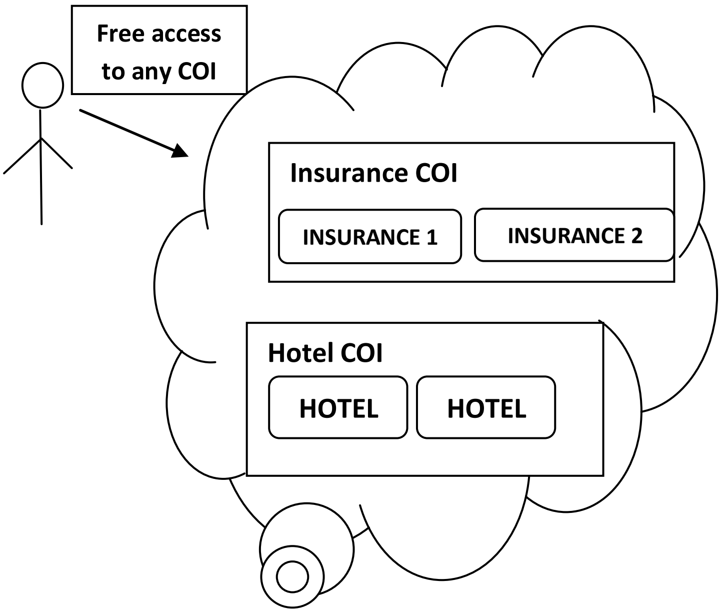

Figure 4 Accessibility of COI classes

For example, initially user A can access hotel 1, hotel 2, insurance 1 or insurance 2. But, when once a user accesses an object of the COI class then it cannot access the CD of the same class. For example, if user A access hotel 1 initially then it cannot access hotel 2 as it is of the same CD of hotel COI class. But it can access insurance 1 or insurance 2 as they belong to different COI class.

This CCWSP restricts the client from accessing the data of multiple conflicting classes. Thus the clients with the same interest or field are not able to gain access to the data of the clients with conflicting interest. If any user/client tries to do so then, it is detected. Thus the proposed CCWP decreases the response time of detection of the internal attacks. The CloudChinese Wall Security Policy (CCWSP) eliminates the possibility of the internal attacks as no client can access objects or data of another client, although they are sharing the same Cloud platform.

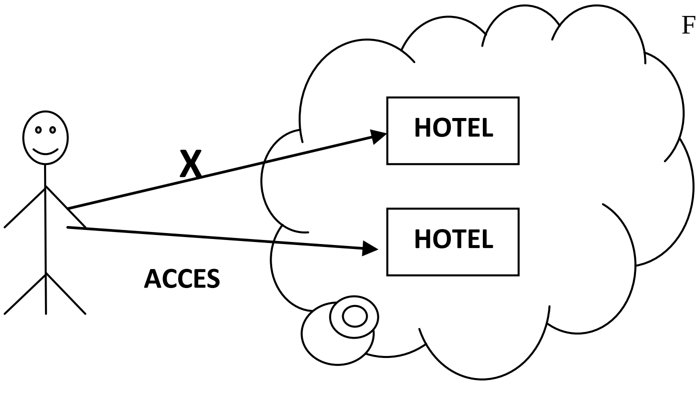

Figure 5Accessibility of CD

Now for Clouds to support the Chinese wall security policy, it is necessary to identify the elements in Clouds which correspond to the various elements of Chinese wall model.

Definition 1: According to CCWSP, a subject is a client who accesses the services or data of the Cloud and let it be denoted by S={s_1, s_2, …..,s_n}.

Definition 2: The nodes of the Clouds are the instances of Clouds which will be denoted by I = {i_1, i_2, ….,i_n}.

Definition 3: The instances of the Cloud are refered to as the objects in the Cloud-based environments and let it be denoted O = {obj_1, obj_2, ….,obj_n}.

Definition 4: The company dataset is the domain from which the multiple instances of a class can be selected.For example all the instances in the LIC company dataset store the data and services associated with LIC. Let it be denoted by CD = {cd_1, cd_2, ….,cd_n}.

Definition 5: The COI class contains multiple company datasets. The classes are built on the basis of the competing clients and business areas. Let it be denoted by C = {c_1,c_2, ….,c_n}.

Consider a set of objects(O) and a set of subjects(S). Objects are items of information related to a company. Subjects are active entities interested in accessing protected objects. Objects related to a single company are part of company dataset(CD). Data sets of companies in the competition are stored in the conflicts of interest(COI) class[13].

The COI(O) refers that object(O) is contained in the COI class and CD(O) refers that object(O) is contained in the company dataset(CD). It is assumed that every object belongs to exactly one conflict of interest (COI)class.

In each COI class (e.g. Hotel), a subject can only read objects in an exceedingly single CD(e.g. Tata). A minimum of (n) subjects area unit are needed to access all objects in an exceedingly COI category with completely n CDs.

Assumptions:

1. No company dataset(CD) can span to more than one COI class. Thus two objects of the common CD will be in the same COI class.

Features:

1. This model is capable to capture the changes over time.
2. It has the capability to track the access history to differentiate between the legal and illegal.
3. This model gives free access of all the objects initially, but once an object is accessed by a subject, then it cannot access any other object of the same COI class.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

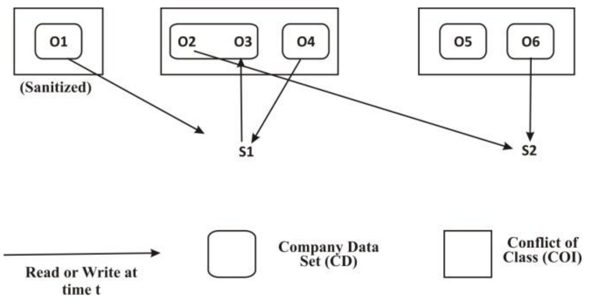

Figure 6 Representation of Subjects and Objects

In the above figure 6, a system is shown which comprises of subjects and objects. Objects are actively accessed by the subjects, while objects are passive entities. In this system only read and write operations are allowed. The direction of the arrow indicates the flow of information.In the read operation direction of flow is from object to the subject. While in the write operation direction of flow is from the subject to the object. The information flow can also be indirect[29].

As shown in the figure 6, the subject s1 reads object o1 and later writes to object o3. Thus, information flows from object o1 to o3.

Every object has a place with acompany dataset. Company datasets are additionally assembled into Conflict of Interest classes. A sanitized object is one which does not have any confidential information. An object with confidential information is called un-sanitized object. Chinese wall security policy is maintained when there are two un-sanitized objects which have a place with various company datasets inside a similar Conflict of Interest class. In this case, information cannot flow from both of these objects to a subject. Sanitized objects are special case as these don't contain any private data at the beginning and flow of data is free.

In the figure 6,amongthe three Conflict of Interest classes,one is sanitized object and the other two are un-sanitized objects. Objects o2 and o3 have a place with a similar company dataset inside a Conflict of Interest class and therefore are not in conflict. Objects o2 and o4 belong to completely different company datasets inside the same Conflict of Interest class are in conflict, and so they requiresecurity from the stream of information. On the off chance that such stream happens, it might abuse the security approach.

Consider an example in the figure 6, if s2 attempts to read o5, then it is not allowed due to the simple security rule. This is due to the fact that s2 has already accessed object o6 for the read operation and both the objects o5 and o6 belong to the same conflict of interest class.

B. Cloud Clark Wilson Policy(CCWP)

In the propose Multilevel Cloud Security Policy(MCSP), the CCWP comes into operation when a client gains access to a CD of any COI class. Now, how the client can operate within that particular CD is determined by the CCWP. The CCWP uses the basic Clark-Wilson model with 5 certification rules and 4 certification rules.

Consider an example in which,

1) An individual A generates a request for a supply. It sends the copies to the supply and receiving divisions.
2) When the individual B in the receiving divisiongets the material, he/she checks it. The original order and delivery form are sent to accounts division after making sure that everything is well.
3) An individual C which is a supplier sends a receipt to the individual D in accounts division. On receiving the receipt, individual D compares the delivery and order forms. Then supplier is issued a cheque.

This example can be presented in terms of constrained data itemswhich can be processedonly by the transformation procedures. Integrity is maintained as only the TPs can alter the data items. The persons A,B, C, and D are the users while the create order, send order, create delivery form, send delivery form, sign delivery form, create invoice, send invoice, and compareinvoice to order are the TPs. Order, delivery form, invoice, and check are the CDIs. Users can invoke the TPs according to their duties. This facilitates the separation of duties.

VI. WORKING OF THE PROPOSED MODEL

As a complete illustration of Multilevel Cloud Security Policy(MCSP), consider that a user Allen tries to access the Cloud services. This Cloud service provider is catering to the needs of hotels Taj and Tata, and Insurance companies LIC and Max(Figure 7). Allen is free to get access to any of the COI class i.e. Hotel or Insurance. If the Allen accesses the hotel Tata then it is not allowed to access the hotel Taj. This is due to the fact that a Cloud Chinese wall is built in the Hotel COI class between the Taj and Tata company dataset. But Allen is allowed to access any CD of Insurance company COI class i.e. LIC or Max.

Now, when once Allen gains access to hotel Tata then, the CCWP becomes operational. Allen will be able to access the data in the Taj class according to his privileges and the rules of CCWP so that the integrity of the system is maintained.

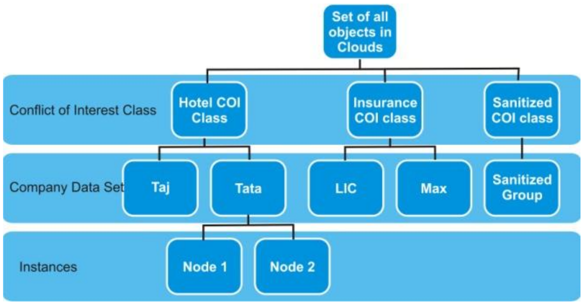

Figure 7. Representation of COI classes, CD

So in this proposed policy, a Chinese wall is formed as the clients once access any CD of any COI. This wall restricts free access to multiple CDs of the same COI class. Cloud Clark policy provides security within the CD.

VII. CONCLUSION

Cloud security is of prime concern for the clients of the Cloud-based environments. Among the various types of attacks like DoS, Replay attack, MIME etc.,the malicious insider attacks are the main focus of this work.

The proposed work aims to enhance the security of Cloud computing to protect the systems and data in the Clouds. The proposed Multilevel Cloud security policy (MCSP) is capable enough to mitigate malicious insider attacks. This policy comprises of Cloud Chinese wall security policy (CCWSP) and Cloud Clark Wilson Policy (CCWP). Future work involves the implementation of this policy on various deployment models of Clouds.

REFRENCES

[1] A. Jain and R. Kumar, “A Taxonomy of Cloud Computing,” *Int. J. Sci. Res. Publ.*, vol. 4, no. 7, pp. 1–5, 2014.

[2] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” *IEEE Comput. Soc.*, pp. 69–73, 2012.

[3] A. Jain and R. Kumar, “Confidentiality Enhanced Security Model for Cloud Environment,” *Proc. Second Int. Conf. Inf. Commun. Technol. Compet. Strateg. - ICTCS ’16*, pp. 1–6, 2016.

[4] P. Oberoi and S. Mittal, *Review of CIDS and techniques of detection of malicious insiders in cloud-based environment*, vol. 729. 2018.

[5] A. Jain and R. Kumar, “Hybrid load balancing approach for cloud environment,” *Int. J. Commun. Networks Distrib. Syst.*, vol. 18, no. 3/4, p. 264, 2017.

[6] P. Oberoi, S. Mittal, and R. Kumar, “ARCN: Authenticated Routing on Cloud Network to Mitigate Insider Attacks on IAAS , unpublished.”

[7] P. Oberoi and S. Mittal, “Survey of various security attacks in clouds based environments,” *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 976, pp. 405–410, 2017.

[8] P. Oberoi, “ADRCN : A Framework to Detect and Mitigate Malicious Insider Attacks in Cloud-Based Environment on IaaS,” *Int. J. Math. Eng. Manag. Sci.*, vol. 4, no. 3, pp. 654–670, 2019.

[9] M. Kandias, N. Virvilis, and D. Gritzalis, “The Insider Threat in Cloud Computing Miltiadis,” *Crit. Inf. Infrastruct. Secur.*, vol. 6983, pp. 93–103, 2013.

[10] Z. M. Yusop and J. H. Abawajy, “Analysis of Insiders Attack Mitigation Strategies,” *Procedia - Soc. Behav. Sci.*, vol. 129, pp. 611–618, 2014.

[11] V. Kessler, “On the {Chinese Wall} Model,” *Eur. Symp. Res. Comput. Secur.*, pp. 39–54, 1992.

[12] A. Kesarwani, C. Gupta, M. M. Tripathi, V. Gupta, R. Gupta, and V. K. Chaurasiya, “Implementation of Chinese wall model in cloud computing for enhanced security,” *Int. Conf. Emerg. Trends Networks Comput. Commun.*, pp. 411–413, 2011.

[13] M. X. Yang, L. N. Yuan, and Z. X. Yang, “A discuss of computer security strategy models,” *2010 Int. Conf. Mach. Learn. Cybern. ICMLC 2010*, vol. 2, no. July, pp. 839–842, 2010.

[14] D. F. C. Brewer and M. Nash, “The Chinese Wall Security Policy,” *IEEE*, pp. 206–214, 1989.

[15] B. Matt, *Introduction to Computer Security*, vol. 91. 2017.

[16] S. Yu, X. Gui, J. Lin, F. Tian, J. Zhao, and M. Dai, “A security-awareness virtual machine management scheme based on Chinese wall policy in cloud computing,” *Sci. World J.*, vol. 2014, 2014.

[17] J. Jin and M. Shen, “Analysis of security models based on multilevel security policy,” *Proc. - 2012 Int. Conf. Manag. e-Commerce e-Government, ICMeCG 2012*, pp. 95–97, 2012.

[18] D. D. Clark and D. R. Wilson, “A Comparision of Commercial and Military Computer Security Policies,” *Proc. Symp. Secur. Priv.*, pp. 184–194, 1987.

[19] J. J. Dougherty, “Interested in learning more ? In sti tu Au th re ns f rig,” *Style (DeKalb, IL)*, no. Security 401, 2011.

[20] M. Anderson, P. Montague, and B. Long, “A context-based integrity framework,” *Proc. - Asia-Pacific Softw. Eng. Conf. APSEC*, vol. 1, pp. 1–9, 2012.

[21] T. Tsai, Y. Chen, H. Huang, P. Huang, and K. Chou, “A Practical Chinese Wall Security Model in Cloud Computing,” *2011 13th Asia-Pacific Netw. Oper. Manag. Symp. Taipei*, p. 1–4., 2011.

[22] X. Ge and F. Polack, “Secure Databases : An Analysis of Clark-Wilson Model in a Database Environment Secure Databases : an Analysis of Clark-Wilson Model in a Database Environment,” no. May 2014, 2004.

[23] S. Fehis and O. Nouali, “A New Distributed Chinese Wall Security Policy Model,” *J. Digit. Forensics, Secur. Law*, vol. 11, no. 4, pp. 149–168, 2016.

[24] S. Alqahtani and R. F. Gamble, “Enforcing the Chinese wall model for tenant conflict of interest in the service cloud Indrakshi Ray,” *Int. J. Bus. Process Integr. Manag.*, vol. 7, no. 2, pp. 166–177, 2014.

[25] W. She, I. Yen, and B. Thuraisingham, “Rule-Based Run-Time Information Flow Control in Service Cloud,” 2011.

[26] R. Wu, G. Ahn, H. Hu, and M. Singhal, “Information flow control in cloud computing,” in *Proceedings of the 6th International ICST Conference on Collaborative Computing: Networking, Applications, Worksharing*, 2012, pp. 1–7.

[27] Q. Shen, X. Yang, X. Yu, P. Sun, Y. Yang, and Z. Wu, “Towards Data Isolation & Collaboration in Storage Cloud,” 2011.

[28] S. Pramanik, V. Sankaranarayanan, and S. Upadhyaya, “Security policies to mitigate insider threat in the document control domain,” *Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC*, pp. 304–313, 2004.

[29] A. Sharifi and M. V. Tripunitara, “Least-restrictive enforcement of the Chinese wall security policy,” *Proc. 18th ACM Symp. Access Control Model. Technol. - SACMAT ’13*, p. 61, 2013.

AUTHORS PROFILE

Ms. PriyaOberoi received her Master’s degree from Maharishi Dayanad University, Rohtak. Presently, pursuing Ph.D. from M.M. (Deemed to be University), Mullana, Ambala, Haryana, India. She is working as Assistant Professor in Department of Computer Science, D.A.V Centenary College, Faridabad. She has 10 publications in International/National Journals and Conferences She is member of Computer Science Teachers Association (CSTA) and International Association of Engineers (IAENG). Her research area includes Network Security, Cloud Computing, Wirelesscommunication and Distributed Environments.

Dr. Sumit Mittal received his Doctorate & Master’s degree from Kurukshetra University, Kurukshetra. Presently, he is working as Professor & Principal at M.M. Institute of Computer Technology & BusinessManagement, M.M. (Deemed to be University), Mullana, Ambala, Haryana, India. Two scholars awarded their Ph.D degree under his supervision and currently 8 scholars are ongoing. He has more than 40 publicationsin International/ National Journals and Conferences. He has chaired number of technical sessions in International/National Conferences. He is a life member ofComputer Society of India. His research area includes Cloud Computing, Computer Architecture, Wirelesscommunication and Distributed Environments.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Dr. Rajneesh Kumar Gujral is working as Professor in the Department of Computer Science & Engineering, M.M. Engineering College, (M. M. Deemed to be University), Mullana, Ambala. He supervised 34 M. Tech, 1 M. Phil and 6 Ph.D research scholars among 6 scholars, four research scholars awarded Ph.D degree in the session 2017-18, and 1 scholar submitted their Ph.D report and 1 is ongoing. He has about 70 publications in International Journals and Conferences. He is also reviewer /TPC member of various IEEE, Scopus and Springer indexed International Journal and Conferences. He is very renowned researcher in his domain area. He has 375 Google citations in his credit and 13.48 research gate score. His research area includes Cloud Computing, Wireless Communications, Mobile Ad hoc & Sensor based Networks and Network Security.