International Journal of Advanced Research in

Computer Networking,Wireless and Mobile Communications

Volume: 2 Issue: 2 15-Apr-2015,ISSN_NO: 2320-7248

Corporate Case Governance in Secure Triple DES Data Changes and Multi Hand Administration

Bhavani.M[1], M.C.Babu[2]
PG Scholar –Department of Computer Science,
Assistant Professor- Department of Computer Science,St.Peters University,Chennai, India.

Abstract **-** *Corporate case governance plays a key role as a management technology for end – to – end, IP-nized networks and telecommunication networks. Policies are rules governing the choices in behaviour of a system. They are often used as a means of implementing flexible and adaptive systems for management of internet services, distributed systems, and security systems. In this paper the modification or change in a Case based on user administration, the Chief vigilance commissioner, vigilance commissioner, secretary (Home Minister) are the members who are involved in a case. Based on the privilege, those peoples are formed under the group of society. Multiple works is handled in a society. Any modification is done based on users in a administration. Here the First user in this society, changes the case in a file .A private key is generated over the case due to the modification done in a file. After modification, user send an email to another user in the administration and public key is generated. Second user having private key already in a file and he accepts the changes over first user means cases both public and private keys are combined. Finally, modification done in a file.*

Keywords: Private key, public key , CBI key and encrypting the data storage

1. INTRODUCTION

Policy-based management has become a promising solution for managing Enterprise-wide networks and distributed systems. The main motivation for the recent interest in policy-based services, networks and security systems is to support dynamic adaptability of behaviour by changing policy without recoding or stopping the system [1]. This implies that it should be possible to dynamically update the policy rules interpreted by distributed entities to modify their behaviour. Policies are rules governing the choices in behaviour of a system [3]. when to perform storage server backups, register new users in a system, or install new software. Authorisation policies are used to define what services or resources a subject (management agent, user or role) can access[5]. In addition, security management policies are needed to define the actions to be taken when security violations, such as a series of login failures occur for a particular user, or an attack on the system is detected. Policies are persistent so that a one-off command to perform an action is not a policy.

Policies define choices in behaviour in terms of the conditions under which predefined operations or actions can be invoked rather than changing the functionality of the actual operations themselves. In today’s Internet-based environments security concerns tend to increase when mobile code mechanisms are introduced to enable such adaptation, and so many researchers favour a more constrained form of rule-based policy adaptation [5]. Large-scale systems may contain millions of users and resources. It is not practical to specify policies relating to individual entities – instead, it must be possible to specify policies relating to groups of entities and also to nested groups such as sections within departments, within sites in different countries in an international organisation. Policies are derived from business goals, service level agreements or trust relationships within or between enterprises

2. SECURITY POLICY

Access control is concerned with permitting only authorised users (subjects) to access services and resources (targets). It limits the activity of legitimate users who have been successfully authenticated. Authorisation or access control policy defines the high-level rules specifying the conditions under which subjects are permitted to access targets [14]. However, in many systems there is no real policy specification, only the implementation in terms of low-level mechanisms such as access control lists. The study of access control has identified a number of useful access control models, which provide a formal representation of security policies and allow the proof of properties about an access control system.

2.1 Discretionary access control (DAC)

The policies restrict access to objects based on the identity of the subjects and/or groups to which they belong. Basic definitions of DAC policies use the access matrix model as a framework for reasoning about the permitted accesses. In the access matrix model the state of the system is defined by a triple (S,O,A), where S is the set of subjects, O is the set of objects and A is the access matrix where rows correspond to subjects, columns correspond to objects and entry A[s,o] reports the privileges of s on .Discretionary policies do not enforce any control on the flow of information once this information is acquired by a process, making it possible for processes to leak information to users not allowed to read it[8].

2.2 Mandatory access control (MAC)

Policies enforce access control on the basis of fixed regulations mandated by a central authority, as typified by the Bell-LaPadula, lattice-based model [13]. Which is used to enforce some fixed mandatory policies regarding the actions that subjects can execute on objects. The Biba model uses similar controls as those used in the Bell-LaPadula model for providing integrity of data [7].

3. RELATED WORK

The policy description language (PDL) is an event-based language from Bell-Labs [11] in which they use the event-condition-action rule paradigm of active databases to define a policy as a function that maps a series of events into a set of actions. The language can be described as a real-time specialised production rule system to define policies.If the event occurs under the condition the action is executed. Policy defined event propositions are expressions of the form: event triggers policy-defined-event if condition which reads: If the event occurs under the condition, the policy-defined-event is triggered [1].

The users having poor channel conditions in a multiple access scenario can transmit jamming signals instead of their message signals to improve the secrecy rates of the users with better channels [9]. The authors studied the case of a single helper who can increase the secrecy capacity or achievable secrecy rate of the legitimate link by sending code words independent of the transmitted messages. When the wireless channels are affected by small-scale fading, the availability of the channel state information (CSI) must be taken into account in designing the helper's strategy [2].The secure transmission with multiple antennas II, the multi-input,multi-output, multieaves dropper(MIMOME) collection of geographically related variations [8].

There are multiple antennas at each of the three terminals, referring to it as the multi-input, multi-output, multi-eavesdropper (MIMOME) channel. The multiple-antenna transmitter is instead replaced by a single-antenna transmitter and a number of single antenna available relay nodes, a two-stage process that exploits interference cancellation at the receiver allows for artificial noise to impinge on the eavesdropper that can be cancelled at the receiver [11]. This approach will In particular, the node with the best fading characteristics takes responsibility for message relaying, while those whose fading will significantly reduce their impact on the desired communication play the role of noise generators [13].

4. PROPOSED SYSTEM

In the existing system the traditional framework of case based management consists of four core components: CDP (Case Decision Point), CEP (Case Enforcement Point), CAP (Case Administration Point) and PR (Case Repository). A well-trained case administrator or group will specify, verify cases in case administration point and deploy the cases in case repository. Case enforcement point takes charge of the decision.

Disadvantage:

We cant take actions on the intruder based on the actions of the intruder. The updation is not efficient in this system and we can retrieve the data easily. Here a Collaborative case Administration (CPA for short) is proposed with the essential idea of CPA is that applications with similar functionalities. Every DBA has to accept the modification whichever had been done in the database. We can protect the data from multi hand administration. Any unauthorized person involves to leak the cases means a SMS notification will sent to the admin directly.

Advantages:

This system take actions on the intruder based upon the actions of the intruder in multiple level of authentication. We can protect the data from multi hand administration

4.1 CASE DEFINE ADMIN MODULE

In general, case can be defined as a course or principle of action adopted or proposed by an organization or individual.

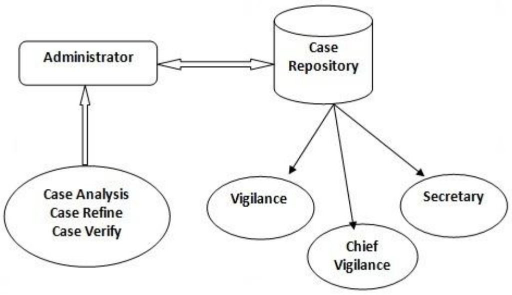


Fig. 4.1 Case Define Admin Module

4.2. LOGIN MODULE

Authentication is the process of determining whether someone or something is. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially using an assigned or self-declared password. An registered user can login into the system through this module.

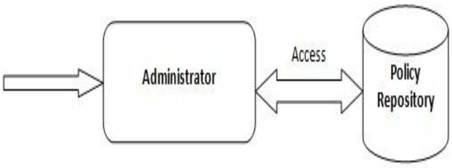


Fig. 2.2. Login Module

4.3. CHIEF VIGILANCE COMMISSIONER APPROVAL MODULE

In chief vigilance commissioner-profile, you face several challenges to providing accurate and complete information while addressing understandable public concerns. In this module chief-vigilance commissioner is having authority to verify the database. Chief-vigilance commissioner having full authority to view and analyze the case and a notification sent to the Admin regarding case analysis.

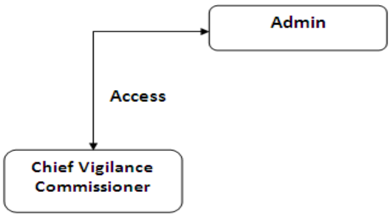


Fig.4.3. Chief Vigilance commissioner approval

4.4. VIGILANCE COMMISSIONER APPROVAL MODULE

Vigilance commissioner doesn’t have full authority to view the case. Half of the information is hided by admin. Vigilance Commissioner plays role next to chief vigilance Commissioner.

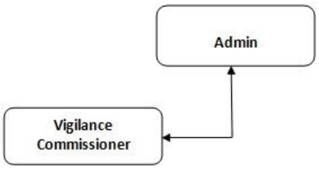


Fig.4.4. Vigilance Commissioner Approval

4.5. SECRETARY APPROVAL MODULE

Secretary checks the information about the case not in detail. Secretary having authority to handle the case with the permission of vigilance and chief-vigilance officer.

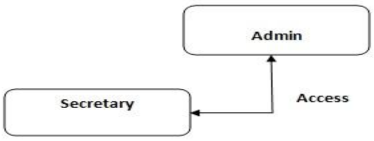


Fig.4.5. Secretary Approval Module

4.6. CASE VIEW ADMIN MODULE

Case-based management of a multi-user workstation typically includes setting individual cases for such things as access to files or applications, various levels of access (Granularity), the appearance and makeup of individual users. The Admin is the authorised role player to define and view the individual case based privileges. The cases generated to the individual roles are viewed on the basis of category. Category based view distinguishes the case in the repository based on the type of category it belongs.

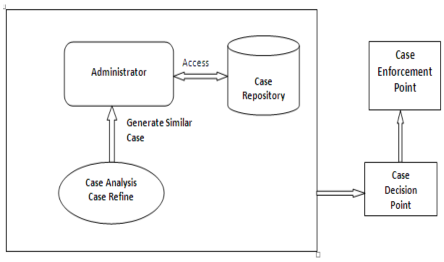


Fig.4.6. Case View

4.7. CBI KEY GENERATION MODULE

In this module three types of administrators having separate private key. If the vigilance levels of people want to delete or modify the database obviously they have to ask permission to chief vigilance commissioner profile people. If the chief vigilance commissioner profile people give acceptance the further queries will be processed. The modifier (admin) are supposed to pass the information with the key to the other admin so as to inform and get permission for proceeding with the modification.

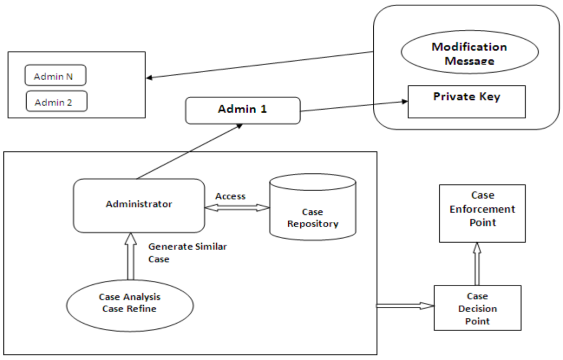


Fig.4.7. CBI KEY Generation

4.8. OBJECT MODIFY MODULE

Case analysis techniques provide the means for assessing case options and recommending the preferred course of action to achieve various organizational, political, social or economic goals. Analysis also provides a way to examine existing cases with an eye toward recommending modifications or improvements.

In this module, the changes that occur in the case are to be monitored by the admin zone using the technique of multi admin handling technique.

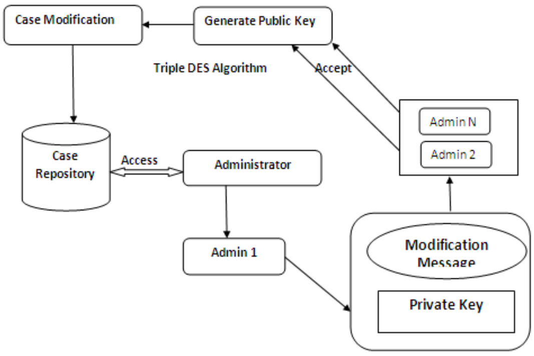
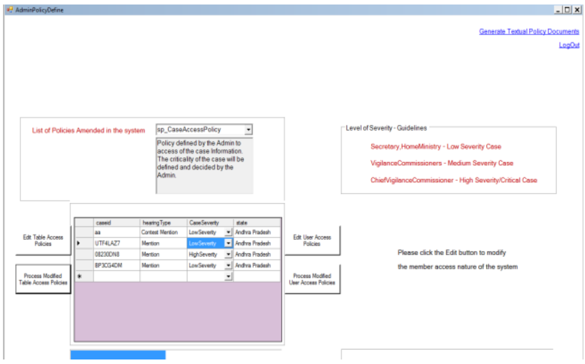


Fig.4.8. Object Modify Module

5. Experimental Results

This result discusses about the implementation of the policy based security for various cases are identified and the below Fig. 5.1., Fig. 5.2. and Fig. 5.3 Shows the implementation of admin policy based on the proposed methodology.


AdminPolicyDefine
Generate Textual Policy Documents
LogOut
Edit Table Access Policies
Process Modified Table Access Policies
Edit User Access Policies
Process Modified User Access Policies

List of Policies Amended in the system: sp_CaseAccessPolicy

Policy defined by the Admin to access of the case Information. The criticality of the case will be defined and decided by the Admin.

Level of Severity - Guidelines

Secretary,HomeMinistry - Low Severity Case

VigilanceCommissioners - Medium Severity Case

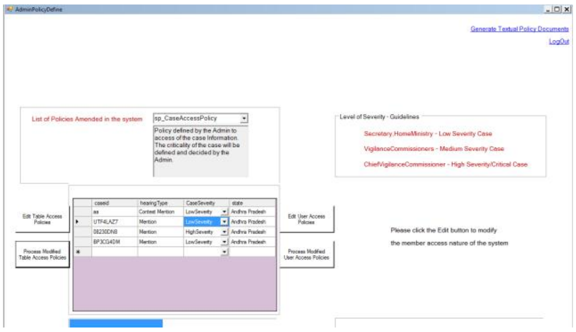
ChiefVigilanceCommissioner - High Severity/Critical Case

caseid	hearingType	CaseSeverity	state
aa	Contest Mention	LowSeverity	Andhra Pradesh
UTF4LAZ7	Mention	LowSeverity	Andhra Pradesh
08230DN8	Mention	HighSeverity	Andhra Pradesh
BP3CG4DM	Mention	LowSeverity	Andhra Pradesh

Please click the Edit button to modify

the member access nature of the system

Fig.5.1. Shows the Admin Policy


AdminPolicyDefine
Generate Textual Policy Documents
LogOut
Level of Severity - Guidelines
Edit Table Access Policies
Process Modified Table Access Policies
Edit User Access Policies
Process Modified User Access Policies

List of Policies Amended in the system: sp_CaseAccessPolicy

Policy defined by the Admin to access of the case Information. The criticality of the case will be defined and decided by the Admin.

Secretary,HomeMinistry - Low Severity Case

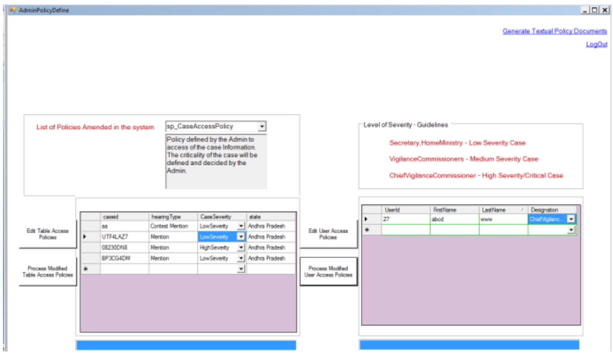
VigilanceCommissioners - Medium Severity Case

ChiefVigilanceCommissioner - High Severity/Critical Case

caseid	hearingType	CaseSeverity	state
aa	Contest Mention	LowSeverity	Andhra Pradesh
UTF4LAZ7	Mention	LowSeverity	Andhra Pradesh
08230DN8	Mention	HighSeverity	Andhra Pradesh
BP3CG4DM	Mention	LowSeverity	Andhra Pradesh

Please click the Edit button to modify the member access nature of the system

Fig.5.2. Table for accessing the policy


AdminPolicyDefine
Generate Textual Policy Documents
LogOut
Level of Severity - Guidelines
Edit Table Access Policies
Process Modified Table Access Policies
Edit User Access Policies
Process Modified User Access Policies

List of Policies Amended in the system: sp_CaseAccessPolicy

Policy defined by the Admin to access of the case Information. The criticality of the case will be defined and decided by the Admin.

Secretary,HomeMinistry - Low Severity Case

VigilanceCommissioners - Medium Severity Case

ChiefVigilanceCommissioner - High Severity/Critical Case

caseid	hearingType	CaseSeverity	state
aa	Contest Mention	LowSeverity	Andhra Pradesh
UTF4LAZ7	Mention	LowSeverity	Andhra Pradesh
08230DN8	Mention	HighSeverity	Andhra Pradesh
BP3CG4DM	Mention	LowSeverity	Andhra Pradesh

UserId	FirstName	LastName	Designation
27	abcd	www	ChiefVigilanc...

Fig.5.3. Edit User Access Policy

6. CONCLUSION & FUTURE WORK

A text mining and the category mining based similarity measure method to obtain similar policies is proposed. This is how the similar policies are fetched and based on that the policies are created. The policy administration is done by generating keys and gets the approval of all the same policy holders before the data is deleted or modified.

Future Enhancement: The safety definition in CPA with a quantified method is investigated. Moreover, we will improve the permission model with finer-grained access control for Android, especially, for INTERNET permission. Finally we will strengthen the mathematics depth of the definitions and analysis of CPA.

Reference

[1]. AHN, G.-J. AND R. SANDHU 1999. The RSL99 Language for Role-based Separation of Duty Constraints. Fourth ACM Workshop on Role-Based Access Control, Fairfax, Virginia, USA, ACM Press.

[2]. Anderson.J.P., Computer Security Technology Planning Study, tech. report ESD-TR-73-51, Mitre, Oct. 1972. Harrison.M.A., Ruzzo.W.L., and Ullman.J.D, “

[3]. ANTÓN, A. I., J. H. DEMPSTER, ET AL. 2000. Deriving Goals from a Use Case Based Requirements Specification for an Electronic Commerce System. Sixth International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ), Stockholm, Sweden.

[4]. Badger.L et al., “Practical Domain and Type Enforcement for UNIX,” Proc. IEEE Symp. Security and Privacy, IEEE CS Press, 1995, pp. 66–77.

[5]. BELL, D. E. AND L. LAPADULA 1973. Secure Computer Systems: Mathematical Foundations and Model. Bedford, MA, MITRE Corporation.

[6]. Barth.A, Felt.A.P, Saxena.P, and Boodman.A. Protecting Browsers from Extension Vulnerabilities. In Proceedings of the 17th Network and Distributed System Security Symposium (NDSS 2010).

[7]. BARKER, S. AND A. ROSENTHAL 2001. Flexible Security Policies in SQL. Fifteenth Annual IFIP WG 11.3 Working Conference on Database and Application Security, Niagara on the Lake, Ontario, Canada.

[8]. Beznosov.K, Inglesant.P, Lobo.J, Reeder.R, and Zurko.M.E. Usability meets access control: challenges and research opportunities. In SACMAT ’09: Proceedings of the 14th ACM symposium on Access control models and technologies, pages 73–74, New York, NY, USA, 2009. ACM.

[9]. BOSWELL, A. 1995. Specification and Validation of a Security Policy Model. IEEE Transacations on Software Engineering 21(2).

[10].Enck.W., Ongtang.M., and McDaniel.P.D., On Lightweight Mobile Phone Application Certification. In E. Al-Shaer, S. Jha, and A. D. Keromytis, editors, ACM Conference on Computer and Communications Security, pages 235–245. ACM, 2009.

[11]. Kohonen.T., Self Organizing Maps. Springer, third edition, 2001. [17], Lampson.B.W., Protection. SIGOPS Oper. Syst. Rev.,8(1):18–24, 1974.

[12]. Krstic.I and Gar!nkel.S.L., “Bitfrost: The One Laptop per Child Security Model,” Proc. Symp. Usable Privacy and Security, ACM Press, 2007, pp. 132–142.

[13]. Li.N., Grosof.B.N., and Feigenbaum.J., “Delegation Logic: A Logic- Based Approach to Distributed Authorization,” ACM Trans. Information and System Security, vol. 6, no.1, 2003, pp. 128–171.

[14]. Ongtang.M., McLaughlin.S.E, Enck.W., and McDaniel.P.D., Semantically rich application-centric security in android. In ACSAC, pages 340–349. IEEE Computer Society, 2009.

[15]. Reeder.R.W., Bauer.L., Cranor.L.F., Reiter.M.K., Bacon.K., How.K., and Strong.H., Expandable grids for visualizingand authoring computer security policies. In CHI ’08, pages 1473–1482, New York, NY, USA, 2008. ACM.

About the Author

Ms.Bhavani.M has completed her B.E., in Computer Science and Engineering from Anna University in 2009 and perusing her Masters in St.Peters University. She is working as a Programmer in IBM Back Office support in Chennai.. Her areas of interest are Networks and Data mining.