ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

A System for Timely and Controlled Information Sharing in Emergency Situations

[I]V.Nivedita, [II]K.Sathya, [III]P.Manjula
[I]ME Student, Computer Science and Engineering, Srinivasan Engineering College
[II]ME Student, Computer Science and Engineering, Srinivasan Engineering College
[III]Head of Department, Information Technology, Srinivasan Engineering College

Abstract
At the time of natural disasters or emergency situations like floods, earthquakes, hurricanes and man-made disasters e.g., airplane crashes, terrorist attacks, nuclear accidents. At this time we ought to manage the emergency situation effectively for that the most essential requirement is the information sharing. In this work I present a framework control model (ie) Access control model which will constrain the controlled information sharing in emergency situations which means it would not make the information to deviate from the controlled path and too will provide the secure information sharing from source to destination during natural disasters and the Administration policies are introduced to reinforce the model flexibility during at the time of emergency situations. The Access control model will have the verifiers to check the information coming from the user is authorized information or not and also will detect the information coming from user whether it is critical or normal emergency situation regarding that it will handle the situations.

Keywords
Access Controls, Privacy, Security, Data Sharing

I. Introduction

The natural catastrophic events, e.g., floods, earthquakes, hurricanes, and man-made disasters such as airplane crashes, terrorist attacks, and nuclear accidents this highlights the need for a more essential emergency management. For example the incident happened in September 11, 2001 have shown that the deficit of information sharing that resulted in the failure of terrorist attacks. This pointed out the need of more effective, timely, and resilient information sharing at the time of emergency management and often require to access the resources during normal operations.
To cope with these needs here proposing an Access control model that is a framework model which reinfoce controlled information sharing in emergency or natural situations. This model is able to constrain flexible information sharing within a single organization though the specification and enforcement of emergency policies. Emergency policies allows the instantiation of temporary access control policies (tacp). It presents an in-depth analysis of the checks performed by the system to make sure policy correctness. The prototype implementation has been extended to implement the correctness validity checks and administration policy enforcement. The key characteristics of the model is that emergencies are specified through events on top of Complex Event Processing (CEP) systems which will find the information whether it is critical or normal situations from the user. A language called Core Event Specification Language (CESP) system which has used to define events describing the beginning/and ending of an emergency. An emergency is the tuple where init and end are emergency events specified in CESL, such that init denotes the event triggering the emergency and end is the optimal event that turns off the emergency. Time-out is the time within the emergency expires even though end has not occurred.

Floods

Earthquakes

Airplanecrashes

Fig. 1: Natural and Man-made Disasters

II. Emergency Information Sharing

A. Basic Idea of Proposed Methodology

A proposed method includes the Access control model to constrain controlled information sharing in emergency situations. There is need for a more masterful, timely, and flexible information sharing at the time of emergency or natural situations. During the emergency there is a often need to access the resources that are not allowed during the normal system operations. It is often the case that specific actions should be performed to manage the emergency. When comes to advantages providing the full security guarantee should be essential , no interference or jamming, and acknowledgement received from this we will make sure that information has reached the destination at a correct time and with security.

B. Emergency Policy Correctness

The main role of emergency policy correctness is constraining the temporary access control policies. It consists of two main steps.

- The making or erasure of the corresponding emergency instances.
- The consequent building or/deletion of the corresponding tacps (temporary access control policies).

The emergency policy correctness comes before the Emergency Handler. The emergency handler includes two steps first step is emergency repository which checks the emergency related to received tuple if any. Then the new emergency instance is created. And the second step is tacp template repository which checks the templates related to activated emergency if any. Then creating the corresponding tacp instance.

C. Simultaneous Holding Problem

The Simultaneous Holding Problem mainly for preprocessing validity check .Let c be a CESL (Core Event Specification Language) is used to define events describing the beginning/ and ending of an emergency events. It also defined as the set of tuples satisfying the event whether event may be normal or critical events. Here proposing two additional strategies to detect the simultaneous holding problem (SHP). The preprocessing validity check is used to detect before the emergency policy registration, if its emergency description might bring to potential SHP so as to prevent its registration in the system. And there is a chance to easily detect that there exist some tuples satisfying simultaneously both init and end events as their validity sets are not disjoint. There is a CEP (Complex Event Processing) which categorizes the emergency information as normal and critical emergencies for example critical emergencies such as Heart Problem, Cancer etc and normal emergencies such as Cold, Ulcer, normal stomach aches etc. After categorizing these events then only events will sent to Emergency Handler.

III. Related Work

The model constrains the fine-grained access control model with attribute level granularity. Many models have been proposed here in support of fine-grained access control from attribute based access control (ABAC). This approach allows team based access control (TMAC) by also integrating contextual information. The Access Control List (ACL) is once the user authenticated that user is allowed to access an application or not depending on whether that user's id is on a list of authorized users can also specify as white lists or unauthorized users can specify as black list.. This mode is either all-in or all-out. It is extremely coarse-grained in the sense that it only considers single dimension, that of the user, defy the modality, actions, and contexts. However it is extremely fine-grained in the sense that it becomes a user specific rule. For example in Coarse: Employees can open the door. Fine: Employees based in the US can open the door during time.

A. Attribute-Based Access Control

In Attribute Based Access Control it uses attributes as building blocks in a structured language and will define and describes access control rules and access request attributes. Instead of defining permissions based on roles only, one should be able to use attributes. Attributes are any bit of data or any label, that depicts a user, modality, aim, thing, environments or action. Anything from an apple, its color, and weight to a person eating that apple, the location of that apple. With Attribute Based Access Control, you can mix and match attributes to define extremely targeted (fine-grained) e.g employees can open the door between 9AM and 10AM or close the door after 5PM if and only if the employee belongs to the door opener group.

The most important requirement is that 1) Coarse: composed of relatively large parts or particles, Loose or rough in texture. 2) Fine: very thin in gauge or texture, not coarse, very small, keen knife with fine edge, very precise or accurate, and trying to be fine. In the Role Based Access Control a user can have multiple roles to which different permissions can be granted. Attribute Based Access Control is a "next generation" authorization model that endow movable, context–aware, and danger-intelligent access control. It will help to obtain masterful regulating the adherence, effective cloud services, deficit time to market for new techniques, and a top down approach to govern through limpidity in policy enforcement. ABAC (Attribute Based Access Control) is a logical access control model that is distinguishable because it control access to objects by evaluating rules against the attribute of the entities actions and the environment relevant to request. ABAC takes RBAC (Role Based Access Control) one step further by providing organizations that provides much greater flexibility and granularity in defining how users can access data with the help of security for that providing an algorithm that is AEP (Advanced Encrption Standard) which is an encryption algorithm for securing the sensitive information. Here the advanced encryption standard purpose is when emergency situations comes such as man-made disasters such as air-plane crashes, terrorist attacks etc at this time of exigency situations have to send the emergency information securely from source to destination then only there won't be any intruders or hackers involved while sending confidential information during exigency situations for this purpose using an Advanced Encryption Standard algorithm to send the confidential information securely. AES is a symmetric depends up on the principle for design also for encryption and it works at multiple network layers at a time. It has a certain block size of 128 bits and key size will be 128, 192, 256 bits.

II. Team-Based Access Control

The Team Based Access Control Model efficiently represents the teamwork in the real world. It will give access some users to unite a team based on their existing roles in some organization within some moderate contexts and novel permissions to do the needed work. In the team based access control between team roles and object types there will be team permission required on both sides and between the team roles as well as team members the user context and object instances will perform the required roles. The role based access control the roles do the particular jobs in an organization. In RBAC single user may play multiple roles at the same or different time in an organization. Multiple users also may play the same role at the same time or at the different times. The user role assignment should be made separately from the role permission assignment. The Role Based Access control has divided in to classes, levels, and domains these three can be grouped in to multiple objects and here using the Bell Lapadula Model.

This model proposed by Thomas at 1997 defines two essential aspects of the collaboration context, users context, and object context. The users context gives a access of knowing the particular users playing a role on a team based access control at any given moment and the object context identifies specific objects needed for collaboration purposes. It gives the advantages of Role Based

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Access Control along with various provisions to setforth the fine-grained access control on individual users in certain roles and on individual object instances. Access Control in collaborative system integrates Role Based Access Control and Team Based Access Control by incorporating context as an entity in architecture. Team Based Access Control looks to include contextual information other than users and object contexts such as time, place and run time binding.

IV. Emergency Policy Administration

A. Emergency Management

It is a discipline of dealing with and avoiding both natural and manmade disasters. The system is intended to preserve people and property from all kinds of endangerous. This can be seen through governmental and nongovernmental organizations such as National Strategy for Homeland Security which shows how individuals and varying levels of government responds during at several phases of disasters. Disaster management does not need to deport the threats themselves though the study and bodment of the threats is an essential of the field.

B. Emergency Scope

An Emergency Scope is a tuple (event, streams, operators) where event {init, end, both}, streams is a group of stream names, and operators is a set of CESL (Complex Event Specification Language) operators. An incidence statement e and an emergency scope emergency scope, we say that e is valid with respect to. emg_scope, if the init (end r both) event is defined on a subset of the streams specified in emergency scope, by using a subsets of CESL operators implied in emg_scope operators.

C. Tacp Scope

A Tacp scope is a tuple (sbj, obj, priv, ctx, obl) where subject, object, context are the subject, object, and context specifications. Priv and obl are a group of allowed privileges and actions respectively.

V. System Architecture

The system architecture shows that how the Emergency information (floods, earthquakes or manmade disasters) sending from source to destination with the security from source to destination at a particular time.

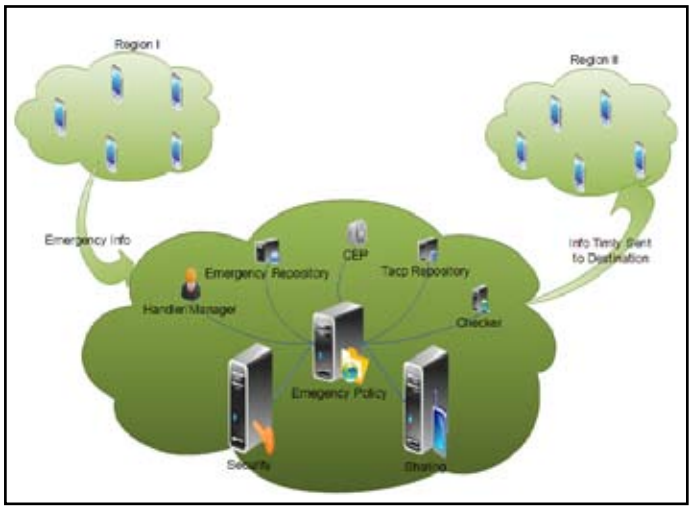

Fig. 2: Overall System Architecture

A. Emergency Policy

The emergency policy also called Access Control Handler which checks the emergency information whether that may be floods, earthquakes, hurricanes, and man-made disasters, e.g airplane crashes, terrorist attacks, nuclear accidents coming from the user is authorized user or not. The Access Control Handler retrieves its profile from the user profile repository which has set of roles authorized to play. Here the main concept is sending the emergency information from source to destination at a particular time. In the system architecture there are two regions take region1 as source and region2 as destination first the region1 (user) sending the emergency information to emergency policy which purpose is to check whether the user is authorized one or not. If the user is authorized person then it goes to Handler/Manager which has only the essential responsibility to handle all emergency information through communication.

B. Emergency Repository

The Emergency Repository comes under the Emergency Handler when the user logs into the system at the time of emergency situation the emergency information goes to access control handler which checks the tuple from the user is authorized or unauthorized. Then goes to Emergency Handler it has two types 1) emergency repository 2) tacp (Temporary access control policy) template repository which stores all kind of emergencies like normal or critical events in the emergency repository.

C. Complex Event Processing (CEP)

The complex event processing which will categorize the events such as normal and critical events. The normal events such as headache, stomachache. The critical events such as heart attack, Blood Pressure (BP). After complex event processing it goes to tacp repository that is temporary access policy. The emergency handler retrieves from the tacp template repository, templates related to activated emergency, if any, by creating the corresponding tacp instance.

VI. Processing of Modules

Here there are four modules have presented the following are.

- Access Control Handler
- Emergency Handler
- Correctness Checker
- Post Processing

A. Access Control Handler

User access, when user successfully logs into the system, the access control handler retrieves its profile from the user profiles repository. This contains profile attributes and set of roles authorized to play. To compute the set of objects is authorized to require the access control handler verifies each regular access control policy in place by returning objects identified by those policies who's authorized to play (roles specified in their subject specification).

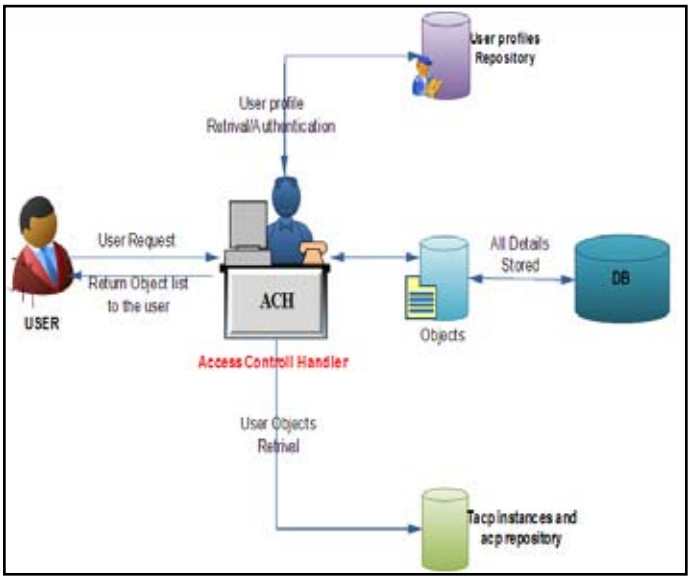

Fig. 3: Access Control Handler

The roles specified in the subject specification include at least a role assigned to. To this set the access control handler also adds objects authorized by tacp (temporary access control policy) instances. The object contained in the tacp instance is returned if subject, object, context conditions in the tacp (temporary access control policy) are satisfied. Finally all the details are stored in to the database. Access Control Handler manages the application wide access control. It is defined through an extensive interface so that alternative implementations can be created. Only one access control handler is active in the server at any time. When the user request to access control handler at the time of emergency situations the profile attributes, objects these list and all collectively stored in the database. Whenever the user comes with the exigency situation tend to meet the authorization process for that information about the user and objects will be in the database. This is the purpose of access control handler.

B. Emergency Handler

Users are send the Emergency Information to CEP (Complex Event Processing) which will categorize the events such as normal and critical events. Once the CEP server receives a tuple (i.e emergency information) triggering an init event, this is immediately will sent to emergency handler. The emergency handler has two process which are emergency repository and tacp (temporary access control policy) template instance. The emergency handler retrieves from the emergency repository the emergency related to received tuple, if any.

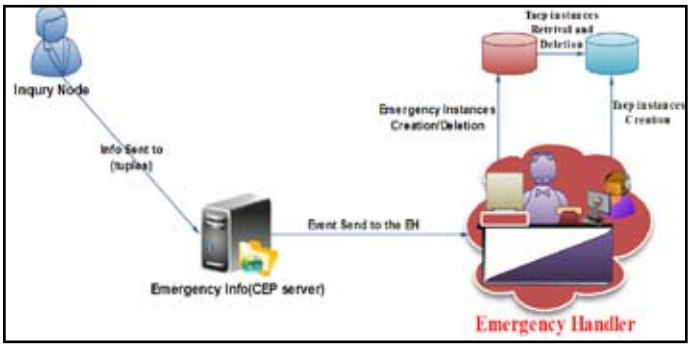

Fig. 4: Emergency Handler

Then the new emergency instance is created unless another emergency instance with the same identifier has been already created (i.e., the emergency policy is already active). Moreover the emergency handler retrieves from the tacp (temporary access control policy) template repository, templates related to activated emergency, if any, by also creating the corresponding tacp instance. When the CEP (Complex Event Processing) server receives any tuple that causes the detection of an event, it sends such a tuple to emergency handler which checks if their exists an emergency an emergency related to it in the emergency repository. If this is the case the corresponding emergency instance and tacp instances are deleted. The inquiry node will enquire the what kind of emergency information comes from the user then it goes to ACH (access control handler) which checks the information comes from the user is authorized or not by checking the profile attributes of user from the user repository which is collectively stored in the database. After this process information will sent to CEP (Complex Event Processing) which will categorize the vents such as normal and critical events and then send to emergency handler which will create the tacp instances if the emergency related to received tuple if any from the mergency repository.

C. Correctness Checker

In correctness checker each time a user defines/modifies the emergency description (i.e., init, and end events) and then to check and monitoring all types of problems. Then the links are verified whether valid or invalid. If invalid the link will be aborted in the process. In the correctness checker the main concept is it will preprocessing validity checks.

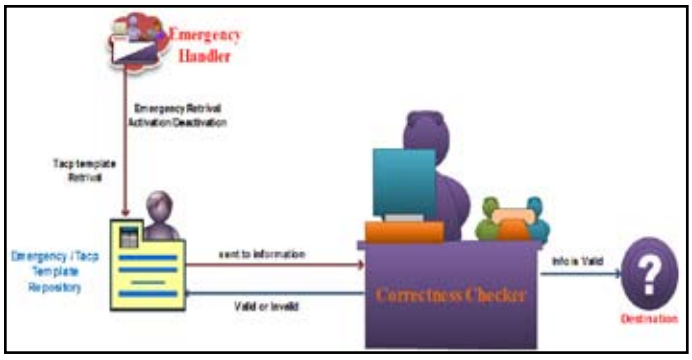

Fig. 5: Correctness Checker

Then the links are verified whether valid or invalid. If invalid the link will be aborted in the process. In the correctness checker the main concept is it will preprocessing validity checks.

VII. Conclusion

In this system an extension of the emergency access control policy has presented with the chance of determining administration policies which are introduced to increase the model flexibility during exigency policies and also the extended version of the prototype has presented. It has carried out an exigency policies into an access control model which is mainly for checks the emergency information whether that may be floods, earthquakes, hurricanes, and man-made disasters such as airplane crashes, terrorist attacks, nuclear accidents coming from the user is authorized one or not this is the purpose of access control model. A correctness checks also has defined to dodge the useless activation/deactivation exigency policies. There is a plan to elaborate this work in to different directions. In the existing system it was done in single organization

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

now doing along in a different directions and to carry out many experiments to evaluate the times needed for administration policy enforcement As a future work in the proposed system plan to make a comparison between static and dynamic template instantiation and goal to enforce information sharing among multiple organizations with avail of cloud computing techniques.

References

[1] *J.G.Alfaro,"Management of Exceptions on Access Control Policies", IEEE Int'l Information Security, pp. 97-108, 2007.*

[2] *C.Ardagna, S.De Capitani Di Vimercati, S.Foresti, T.Grandison,"Access Control for Smarter Healthcare Using Space Policies", Computers and Security, vol. 29, pp. 848-858, 2010.*

[3] *M.Y.Becker,"A Formal Security Policy For an NHS Electronic Health Record Service", Technical Report UCAM-CL-TR-628,Computer laboratory, University of Cambridge, Mar-2005.*

[4] *M.Y.Becker,P.Sewell,"Cassandra:Flexible Health Trust Management, Applied to Health Records", IEEE CS 17th Foundations Workshop (CSFW), 2007.*

[5] *B.Carminati, E.Ferrari, G.Guglielmi,"Secure Information Sharing on Support of Emergency Management", IEEE Int'l Conf.Social Computing, 2011.*

[6] *B.Brucker, D.Hutter,"Information Flow in Disaster Management Systems", IEEE Int'l Conf.Reliability, Availability, Security, 2010.*

[7] *A.Ferriera,D.Chadwick,G.Zoa,"How to Securely Break into RBAC", IEEE 19th Symp Computer Based Medical Systems, pp. 847-857, 2006.*

[8] *E.Freudenthal, T.Pesin, L.Port,"Distributed Role Based Access Control for Dynamic Coalition Environments", IEEE Int'l Conf. Distributed Computing Systems, 2002.*

[9] *D.R.Kuhn, E.J.Coyne,"Adding Attributes to Role Based Access Control", Vol. 43, No. 6, June 2010.*

[10] *H.K.Lee, H.Leudemann,"Lightweight Decentralized Authorization Model for Interdomain Collaborations", Proc ACM Workshop Secure web Services, pp. 83-89, 2007.*