Detection of Unspecified Emergencies Using Controlled Information Sharing

[1] Karan Balasubramanian B.E., [2] Jefferd Jerald B.E.,
[1][2] Department of Computer Science and Engineering
Sathyabama University, Chennai
[1] Karansai1994@yahoo.com

Abstract: **During Emergency situations in the Health care Domain, one of the main work is to manage the situation effectively the most essential requirement for handling the situation is sharing information. In this work, I present a flexible access Control Framework exploiting the complex event processing (CEP) technology which will constraint the controlled information sharing in the health care domain emergency situations. The main aim of this idea is to detect the emergencies that cannot be predicted by anomaly detection techniques, denied access request analysis and analysis of the history of permitted access requests.**

***Keywords*:- Data sharing, Access control, Emergency Management, Security.**

I. INTRODUCTION

The natural catastrophic events, e.g. heart attacks or stroke, sudden difficulty in breathing, sudden loss of consciousness. This highlights the need for a more essential emergency management. For supporting the information sharing in emergency situations, I have defined a flexible access control framework exploiting the Complex Event Processing technology to predict the emergency situations. when an emergency is detected every time ,sets of temporary access control policies are activated. the regular policies are overridden by the access control policies during the emergencies ,allowing first responders the access to information needed during emergency recovery phases. In the model proposed before is able to only cover emergencies that have been specified a priority for a single person .In contrast there are many scenarios where the emergencies cannot be predicted before .In the health care domain ,it is hard to find that if any possible diseases or injuries which might become an emergency and these emergencies are not detected by the system which is not able to be prepared to possible new information needs as this leads to consequences like endangering human lives. The main characteristic of the model is that emergencies are defined 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.

II. EMERGENCY INFORMATION SHARING

A. *Basic Idea of Proposed Methodology*

During emergency situations, the proposed method involves the access control policies to constrain the controlled information sharing .The main aim of this project is by using the wearable devices predicting the unspecified emergency of an abnormal person and to create an XML Based Temproary Access Control Policy for emergency detection.For intimating doctors and relatives we create a mobile application regarding the emergencies and getting timley help.At the time of emergency ,flexible information sharing, more masterful and timely is needed. In this proposed system, the Emergency situations are detected by the TemproaryAccess Control policy (TACP).Complex Event Processing server is used to continuously monitor the health condition of the patients and it also detects the abnormal conditions of the patients.To monitor the patient’s (Temperature , pulse, heart beats), sensor kit (Wearable devices) is used.it detects the emergencies that cannot be predicted and it communicates about the emergencies to the doctor and to the relatives when the patient is alone and the doctor generates the patients report using emergency mobile application and sends the first aid to be done to the patients relatives through a message (sms).An event type is automatically generated according to the values of the patient when an emergency situation is detected .In proposed system ,the doctors have an access control so that the patient records can be accessed based on the disease of patient where the doctor is specialist about the disease.Proposed system also predicts the lung cancer by symptoms tree traversal technique.

B. Emergency Policy Correctness

Constraining the temporary access control policies is one of the main role of emergency policy correctness .It involves two steps.

- ❖ The making or erasure of the corresponding emergency instances

The consequent building or/deletion of the corresponding tacps.

The Emergency Handler comes after the Emergency policy correctness. It includes two steps , the first step is Emergency repository which checks the emergency related to received tuple if any which leads to the creation of emergency instance. The second step is tacptemplate repository which sees the templates relates to the defined emergency if any then creating the corresponding tacp instance.

III. PROCESSING OF MODULES

Here, 4 Modules have been presented ,the following are

- ❖ Registration and Patient Monitoring.
- ❖ CEP Server
- ❖ TACP
- ❖ Emergency Mobile Applictaion

A. REGISTRATION AND PATIENT MONITORING

In this module, the patient and doctor should be register with our web application.Cep server is used to monitor the patient. Once the patient is registered, the Patient ID will be automatically updated in an cep server and all the patient health condition are continuously monitored by the complex event processing server.Cep server is used to detect the abnormal condition of the Patient .

B. CEP SERVER

Whenever emergency is detected, the patients details are separately maintained on the cep server .Each patient have a unique login and once they are logged in our application, they will be able to see the continuous monitoring values of that patient .once the emergency is detected they will be able to see the type of emergencies and also policy type. the emergency policies are also dynamically updated by the hospital administration. The policies are maintained based on the XML.

C.TACP:

Once the emergency is detected, the abnormal patient values are sent to the tacp (temporary access control policies).In that tacp,the policy will be checked based on the patient abnormal values and tacp will detect the type of policy and redirect that patient abnormal values and it will choose the doctor based on the policy type and gives the read or write permission to that specialist doctor in the hospital. The admin has the ability to see all the patient details and also the emergency policy type of the each patient .

D.EMERGENCY MOBILE APPLICATION

After the emergency is detected by the temporary access control policies , that patient's emergency policy and also the abnormal values of the patient are send to the doctor mobile by sums and also to the patient relative mobile number. Once the doctor has received the message by SMS ,the Hospital android application will automatically be opened and the details about the patient and emergency policies are displayed in that application and also application will be automatically opened for patient relative too .After viewing the patient details , the doctor will send the Prescription to the patient relative mobile number .

IV. RELATED WORK

In many domains, the emergency management involves a deep investigation. These three plays a major role during emergency management .The increased usage of social media has lead to revitalization on Emergency management as found in the recent researches where this helps in gaining the public attention by creating awareness .The main goal of this paper is to have a controlled information sharing during emergency situations. Our proposal deals with the access control mechanisms which is the most common way to make sure the sharing of information. In general ,the access control permits the access of data based on the authorizations set which is fixed by the security administrators according to the policies maintained by the access control of the organization.

Based on our knowledge ,only some works have depicted the investigation of information sharing problem during the emergency management where most focuses the access control model .The focus of the current paper is about the management and detection of unspecified emergencies.During emergency situations , the temporary access control policies are activated by the (RBAC) role based access control. Our paper is also related to the models based on BREAK THE GLASS POLICIES (BIG)Which was introduced to avoid the system halts caused by denied accesses. The main idea is that (BIG) policies which makes the regular policies to be overridden by the user. Many works based on BIG have been done.

One is the BIG based on the levels of emergency,that is based on the levels the policies have been classified. Ferreira et al. who showed the first approach to BIG according to temporary accounts permitted with powerful access rights and much more detailed logging.
Like the BIG, this model also supports the access control violations but in a much Safer way. But the BIG involves policies that might lead the systems to unsafe state because it lets its users to break the glass whenever they want .In our proposed system, the violations are controlled and decided by the system and allows flexibility in allowing the violations in a controlled manner.

V. CONCLUSION

In Our Paper, the framework has been proposed to compromise with unspecified emergencies .In this framework, the Emergency access control policies are provided with an extension for determining a chance to increase the flexibility of the model. We have also planned to introduce and develop new techniques to define new and advanced emergency policies automatically .Finally, we have planned to test our framework in the Real world.

REFERENCES

[1] LorenaCazorla, Cristina Alcaraz, and Javier Lopez. Towards automatic critical infrastructure protection through machine learning. In Eric Luiijf and Pieter Hartel, editors, Critical Information Infrastructures Security, volume 8328 of Lecture Notes in Computer Science.

[2] JanaBauckmann, Ulf Leser, Felix Naumann, and Veronique Tietz. Efficiently detecting inclusion dependencies. In In Int. Conf. on Data Engineering (ICDE 07). Poster, 2007.

[3] Alexandra Rostin, Oliver Albrecht, Jana Bauckmannr. A machine learning approach to foreign key discovery

[4] Eamonn Keogh, Jessica Lin, and Ada Fu. Hot sax: Efficiently finding the most unusual time series subsequence. USA, 2005.IEEE Computer Society.

[5] M. S. Beigi, S.-F.Chang, S. Ebadollahi, and D. C. Verma. Anomaly detection in information streams without prior domain knowledge. IBM J. Res. Dev., 55(5):550–560, September 2011.

[6] Ma'ayanGafny, AsafShabtai, LiorRokach, and Yuval Elovici. Detecting data misuse by applying context-based data linkageThreats '10, pages 3–12, New York, NY, USA, 2010.

[7] M. A. C. Dekker and S. Etalle.Audit-based access control for electronic health records.Electron. Notes Theor. Comput. Sci., 168:221–236, February 2007.

[8] Nabil R. Adam, Vijay Atluri, Soon Ae Chun,. Secure information sharing and analysis for effective emergency management. dg.o '08, pages 407–408, 2008.

[9] Claudio A. Ardagna, Sabrina De Capitani Di Vimer. Access control for smarter healthcare using policy spaces.Comput.Secur., 29(8):848–858, November 2010

[10] A Ferreira, R Cruz-Correia, ,". How to break access control in a controlled manner." Washington, DC, USA, 2006. IEEE Computer Society.