Active Rule Based Complex Event Processing For Emergency Management System

[1]Dr.M.Senthil Kumar, [2]M. Sumithra
[1]Associate Professor, [2]P.G Scholar
Department of Computer Science and Engineering
Valliammai Engineering College, Tamil Nadu, India

***Abstract*—A key role of emergency management system is to provide information sharing during an emergency situation . If emergencies are specified beforehand, then it is possible to share information in prior. Whereas in other case like unspecified emergencies like arrhythmia, cardiovascular abnormal heart rate etc..., it is impossible for taking sudden precautions. So in such emergency cases we present a model able to deal with unspecified emergencies. In this paper we provided with a technique which helps us to detect the event using certain active rules called active rule based complex event processing. Temporary access control analysis overrides regular policies during emergency situations. We also defined measures to check whether denied access request is close to unspecified emergency or attempted abuse.our proposed system focus on unspecified emergencies similar to registered emergencies. Although, both are different they possess similar access request and information sharing. After the emergency detected by the temporary access control policies, that patient emergency policy and also the abnormal values of the patient are sent to the doctor mobile by SMS and also to the patient relative mobile number via emergency management application.**

***Index Terms*—Information Sharing, Emergency management system, temporary access control, Active rule CEP.**

I. INTRODUCTION

Information sharing could be a crucial component of any emergency management strategy [1] [2]. The lack of data sharing among concerned agencies resulted in an ineffective emergency management inflicting loss of human lives. To permit versatile data sharing throughout emergency situations, avoiding the danger of data leakage, we have a tendency to outlined a model ready to link further access control policies, besides the regular ones, to the happening of a specific emergency. These policies are known as emergency policies.

Active rules based complex event process monitors patient\'s vital values in real time.Active rules in ACEP alter us to specify a pattern query\'s dynamic condition and real-time actions. The technical challenge is to handle interactions between queries and reactions to queries inside the high-volume stream execution. Therefore, whenever an emergency is detected a group of temporary access control policies (tacps) is activated presumably requiring a group of emergency obligations to be fulfilled. Tacps are access control policies that override regular policies throughout emergency situation. In emergency management eventualities, it\'s common that the consultants of the sector based on response plans,supported regulations and laws as well as on reports ensuing by the emergency preparation and risk assessment section . All these documents represent a solid base from that emergencies and emergency policies may be given.

However, there are several eventualities wherever this can be not enough, since it\'s tough to a-priori work out all potential emergency things. This could have serious consequences, therein one emergencies don\'t seem to be lined by outlining policies and so the system isn\'t ready to reply to their data desires, unless somebody manually triggers the emergency standing. This is often the concept behind the break-the-glass model . However, we have a tendency to believe that the danger of data leakage caused by property the user indiscriminately, breaking the glass [9] [10] may seriously impact the system security. For this reason, during this paper, we have a tendency to explore an alternate approach to alter one emergencies extremely reducing the danger of data escape. The fundamental plan is to open the system to some access management violations, i.e., to grant access to some requests that ordinarily ought to be denied, however that will be permissible because of the happening of an one emergency. The explanation behind this selection is that the danger of information leakage generated by these violations can be below the injury caused by a late emergency response. Obviously, not all denied access requests need to be allowed. In distinction, the concept is to possess a system open solely to those denied access requests that are blocked because of the absence of correct emergency policies. The matter is a way to find whether or not a denied access request (dar in what follows) is said in an one emergency or it\'s merely attempted abuse.

In this paper, we target emergencies that have been kind of like emergency situation already registered within the system. Indeed, though the emergencies are totally different, they need similar -information desires and similar access requests. Therefore, we have a tendency to outline a live to represent, however shut a dar is to satisfy a tacp. We have a tendency to decision this live tacp-dar satisfaction level and a knowledge structure ready to build satisfaction level computation very efficient. Finally, we have a tendency to through an experiment evaluated the effectiveness of our measures in step with totally different dimensions.

II. COMPLEX EVENT PROCESSING

In this section , we explain about basic concepts behind complex event processing without any integration. Complex event processing includes event instances, event types, event streams and pattern queries.

A. Event Instances

Each event instance denotes an immediate occurrence of interest. Input streams of events are called input events which are assumed to be primitive. Every event stream consists of two time stamps, namely application time and system time. The application time for an event instance relate to the discrete moment of the occurrence of event enrolled by the event source.

B. Event Types

Event instances which are similar is grouped under one type called event types. Event types are differentiated with the help of event names. An event type includes associated event schema that defines a set of attributes.

C. Event streams

The input to the ACEP system is a possibly infinite event stream that contains all events of interest. The event stream is heterogeneous, being populated with event instances of different event types.

D. Pattern queries

Pattern queries are a common feature among most of the event processing technologies. Sequence (SEQ) pattern specifies a particular order in which the events of interest must occur.

Complex event processing processes the event of streams by collecting them from various sources to produce output streams. Complex event processing consists of Complex event processing engine and stream processing engine. It is shown in FIG 1.

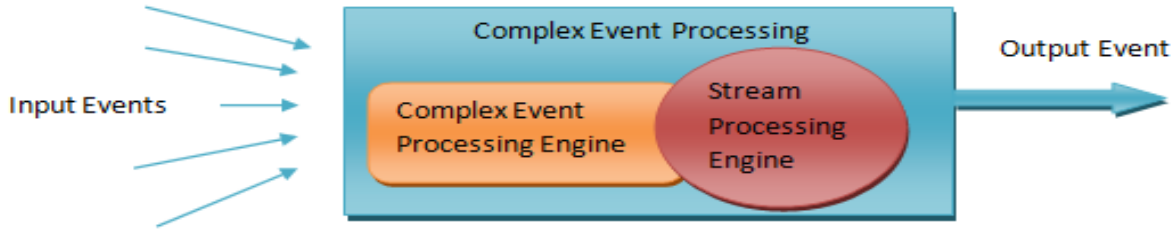

FIG 1: COMPLEX EVENT PROCESSING

III. ACTIVE RULE COMPLEX EVENT PROCESSING

Active Rule Complex Event processing [11] section includes models and architecture of Active rule CEP. Complex event processing provides effective pattern matching on event streams, whereas in real time opportunities and risk detection capability are limited. To overcome this, An integrated model of complex event processing to active rule is known as Active complex event processing (ACEP) is developed. ACEP provides fine grained and more efficient rule processing.

A. Model of Active rule CEP

Our Active rule based CEP focuses on core semantics followed by Event Condition Action (ECA) format. It includes following core semantics namely event triggering, condition and action.In event triggering, SEQ operator is used for triggering the active rules during the process of Active rule Complex Event Processing system change.Condition is a logical test based evaluation of pattern query qualification. If it is true, then action can be performed by the active rule otherwise no action is carried out by active rule.Action in Active rule Complex Event Processing (ACEP) supports write operation on a shared store without affecting the successive pattern query execution.

B. Active rule CEP Architecture

The architecture of Active Rule Complex Event Processing (ACEP) considers loosely coupled and built in.
In a loosely coupled system, CEP engine is considered as a black box for executing pattern queries. The kernel of the engine remains unchanged. Complex event processing technology only provides pattern matching service. Whereas several extensions are added in order to make to perform the full functionality of Active rule Complex Event Processing (ACEP). In Britain, a novel architecture is used. It directly realizes active rule, functionally as part of complex event processing instead of adding on top of CEP engine like loosely coupled software component.

A typical approach is enabled in ACEP to cope with interactions between coinciding accesses and updates is to enforce concurrency management. However, existing concurrency management schedulers square measure supported the notion of an info dealings the execution of a finite sequence of one-time knowledge manipulation operations on typical keeps knowledge sets.

Active Rule primarily based CEP includes question arrange and rule process techniques. A query process in ACEP includes knowledge flow pipeline of stream operators, which has SEQ, window, static-predicate, active-predicate, result construction. The state of ACEP is often modified in accordance with raw event data. The SEQ engage a non deterministic finite automata (NFA) for pattern recovery. This is shown in FIG 2.

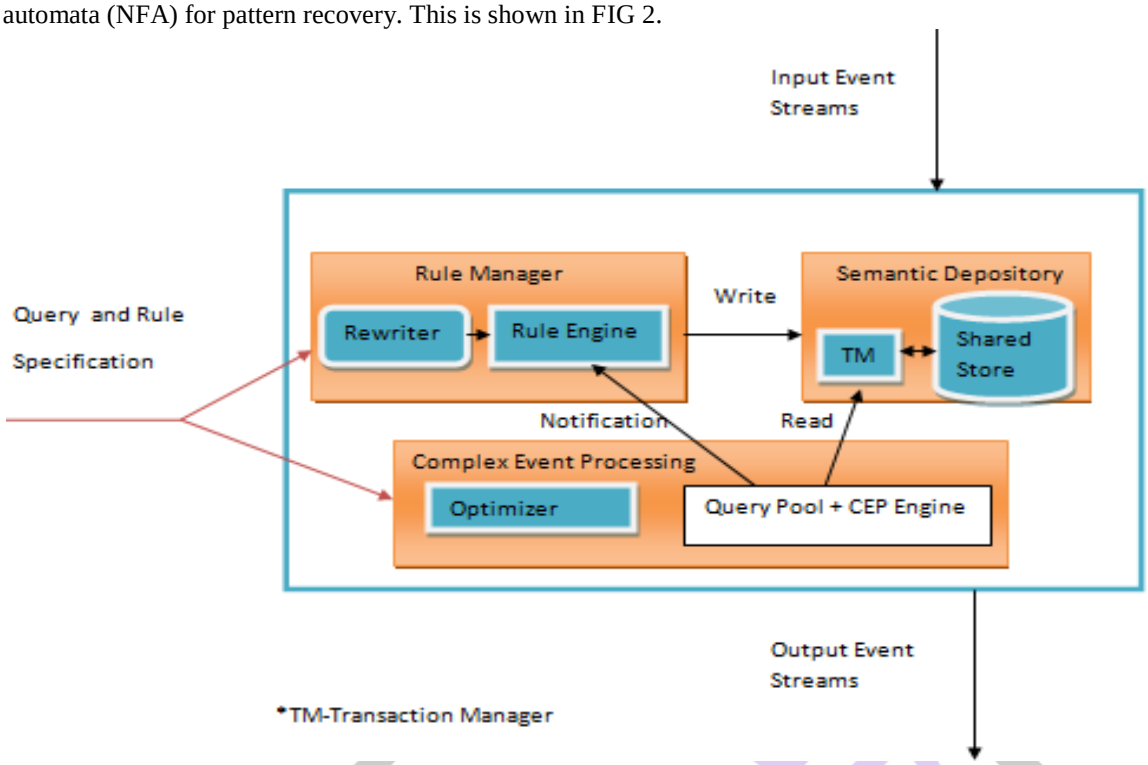

FIG 2: ACTIVE RULE CEP (ACEP)

Rule Manager

Rule manager is tightly integrated with the CEP processor.The rule rewriter co-works with the query optimizer to convert a rule into an alternate, potentially more economical form. Rule event detection is implemented by placing the checking and notification code inside the kernel of the CEP Processor. The rule scheduler executes a triggered rule's action, which directly affects the semantic repository and the CEP processor.

Semantic depository

Semantics Repository is responsible for maintaining the contextual knowledge model that captures relevant information about the environment into which the application is deployed. The semantic knowledge in the semantic repository can be either static or dynamic.

Complex Event Processing(CEP)

Complex Event Processor supports long-running pattern matching queries with negation, nested query and spatiotemporal features over event streams. The processor in our system also handles CEP queries that integrate relational database lookup, typically access to the semantic repository. Queries issued by the application are rewritten by the query optimizer using plan based cost estimation, and then passed to the CEP engine for execution.

In this work, we have a tendency to fill this void by introducing the notion of a dealings within the stream context. Moreover the transitional pattern question process deals with interactions among continuous queries and active rules. This process is particularly difficult as a result of concurrency management poses strict time-based constraints, whereas our algorithms got to work for high-volume streams nonetheless come through near-real-time responsiveness.

Active Rules

Active rules in our system must be able to respond to complex events being detected by CEP queries, semantic information being updated and more generally to any possible CEP system change. Hence the semantics for an Active CEP rule is defined as a function that maps a CEP system change and a CEP system state into the new CEP system state that results from processing those rules Formally, let R be the domain of rules. If r is a rule in R, then r is a function that takes as arguments a CEP system change δ and a CEP system state s. It returns a boolean value, a new set of changes and a new system state; that is:

$r : \Delta \times S \rightarrow \{true, false\} \times \Delta \times S.$

IV. EMERGENCY MANAGEMENT SPECIFICATION

An emergency policy aims to create emergency managers able to state the access control policies that got to be in situ throughout response and recovery. to the current purpose, we tend to style associate degree emergency policy specified it

identifies each the temporary access control policies to be activated and therefore the emergency that has got to trigger their activations. Additional exactly, the associate degree emergency policy specifies the guide of the temporary access control policy that has got to be enforced throughout the emergency. Once associate degree emergency happens, an associate degree instance of the corresponding temporary access control policy guide is formed and keep among regular access control policies. In process temporary access control policy templates associate degrees their association with an emergency, the emergency manager has to be able to specify conditions on values extracted from context in addition as emergency instances. For instance, the temporary access management policy will grant the access solely to the Electronic Management Record (EMR) of the patient that the emergency is instantiated and solely to the paramedic who answered the emergency decision.Emergency Policy identifies both temporary access control policy to be activated and the emergency that has to trigger their activation.

Temporary Access control specification template

TACP template contains tuples such as subject(sbj),object(obj),priveledge(priv) ,expression(exp) with following semantic when the exp boolean expression on context is true,users identified by the subject specification sbj are authorized to exercise the priv priveledge on the protection object obj.In case obj is not null it denotes a set of actions that must be fullfilled everytime an authorized user exercises priv on obj.

Emergency Correctness

Emergency Correctness enable us to check the simultaneously occurred events by using init and end.Init represents the the initilization of event whereas termination of event is represented as end.During emergency correctness we able to detect the wrong correlation between init and end.

V. EMERGENCY MANAGEMENT SYSTEM

Emergency Management System (FIG 3) [3] includes patient's and doctor's registration.Patient's vital value detected by the sensor is send to active rule based complex event processing.temporary access control analyzer triggers emergency management policies as soon as the emergency situation is detected.Emergency Management application is used to provide emergency details to the patient's relative and Patient's doctor.

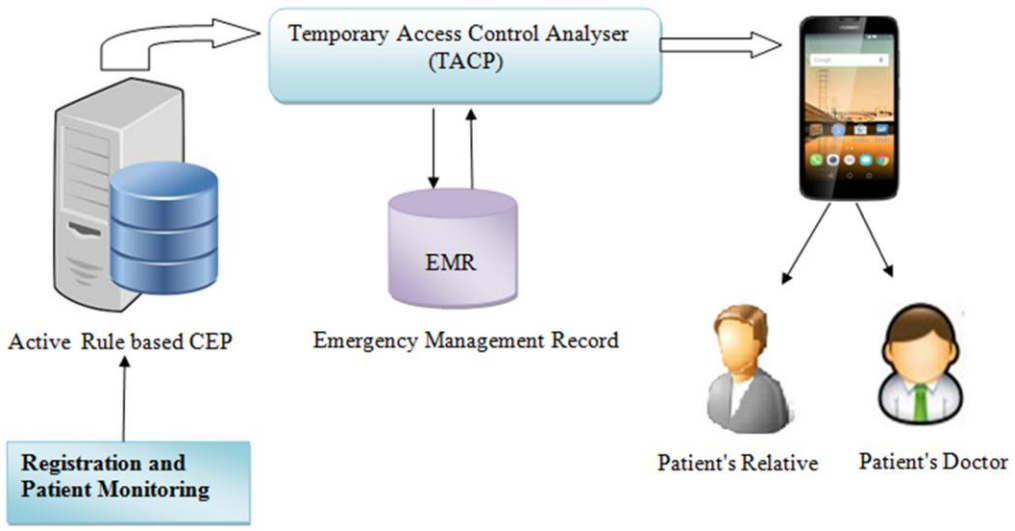

FIG 3: EMERGENCY MANAGEMENT SYSTEM

Registration and Patient Monitoring

The patient and the doctor should be register with Emergency Management System. ACep server is used to monitor the patient. Once the patient 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).Cep Server is used to detect the abnormal condition of the patient.

ACEP Server

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

TACP

once the emergency detected, the abnormal patient values are sent to the tacp (temporary access control policy).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.

Emergency Mobile Application

After the emergency detected by the temporary access control policies, that patient emergency policy and also the abnormal values of the patient are sent to the doctor mobile by SMS and also to the patient relative mobile number. After receiving the SMS by doctor, the hospital android application will automatically opened and the details about the patient and emergency policy 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.

Experimental Setup

Consider a patient being registered and monitored by a emergency management system.Patient vital values are calculated with help of sensor accessed through bluetooth.The application used for accessing sensor is known as healthcare management application.The patient's vital values from patient's are monitored by the use oa Active rule based complex event Processing.

Active Rule based event Processing provides real time monitoring setup for detection of abnormal event occurrence in patient's vital signs. Active rule Complex Event Processing provides efficient processing of queries in real-time, which monitors events detected by sensor.Emergency policies are capable of expressing complex emergency situations, override regular policies with temporary access control policies throughout these situations and support obligations.

Temporary access control analyzer triggers an emergency management process as soon as the emergency situation is detected.TACP analyses the emergency management record for patient's details.Then details about patient is send to the patient's relatives and ptient's doctor via emergency management application.

VI. CONCLUSION

In this paper, emergency policies enable us to manage a versatile and secure information sharing throughout emergency situations.Active rule Complex Event Processing provides efficient processing of queries in real-time, which monitors events detected by sensor.Emergency policies are capable of expressing complex emergency situations, override regular policies with temporary access control policies throughout these situations and support obligations.

REFERENCES

[1] Barbara Carminati, Elena Ferrari, and Michele Guglielmi. A system for timely and controlled information sharing in emergency situations. IEEE Transactions on Dependable and Secure Computing (TDSC), 10(3):129–142, 2013.

[2] Barbara Carminati, Elena Ferrari, and Michele Guglielmi. Controlled information sharing for unspecified emergencies. In International Conference on Risks and Security of Internet and Systems, Oct. 2013.

[3] Damon P. Coppola George D. Haddow, Jane A. Bullock. Introduction to Emergency Management. Butterworth-Heinemann., 2013.

[4] Lemuria Carter, Jason Bennett Thatcher, and Ryan Wright. Social media and emergency management: Exploring state and local tweets. In Proceedings of the 2014 47th Hawaii International Conference on System Sciences, HICSS ’14, pages 1968–1977, Washington, DC, USA, 2014. IEEE Computer Society.

[5] Daniela Pohl, Abdelhamid Bouchachia, and Hermann Hellwagner. Automatic sub-event detection in emergency management using social media. In Proceedings of the 21st International Conference Companion on World Wide Web, WWW ’12 Companion, pages 683–686, New York, NY, USA, 2012. ACM.

[6] Dave Yates and Scott Paquette. Emergency knowledge management and social media technologies: A case study of the 2010 haitian earthquake. Int. J. Inf. Manag., 31(1):6–13, February 2011.

[7] David F. Ferraiolo, Ravi S. Sandhu, Serban I. Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. Proposed NIST standard for role-based access control. ACM Trans. Inf. Syst. Secur., 4(3):224– 274, 2001.

[8] Security and Privacy Committee (SPC). Break-glass: An approach to granting emergency access to healthcare systems. Technical report, White paper, Joint NEMA/COCIR/JIRA, 2004.

[9] Ana Ferreira, David Chadwick, Pedro Farinha, Ricardo Correia, Gansen Zao, Rui Chilro, and Luis Antunes. How to securely break into rbac: The btg-rbac model. In Proceedings of the 2009 Annual Computer Security Applications Conference, ACSAC ’09, pages 23– 31, Washington, DC, USA, 2009. IEEE Computer Society.

[10] A Ferreira, R Cruz-Correia, L Antunes, P Farinha, E Oliveira- Palhares, D W. Chadwick, and A Costa-Pereira. How to break access control in a controlled manner. In Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems, CBMS ’06, pages 847–854, Washington, DC, USA, 2006. IEEE Computer Society.

[11] Di Wang,ElkeRundensteiner,RichardT.Ellison,Han Wang ,”Active Complex Event Processing Infrastructure:Monitoring And Reacting To Event Streamas”, 2011.