www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 3 March 2017, Page No. 20687-20693
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i3.52

Policy Based Detection during Emergency and Sharing Secure Information

K.Akshaya[#1], S.Anu Priya[#2], I.Ashwini[#3], Mrs.Devi*[4]
[#]Student (B.E), [*]Assistant Professor (Grade-1)
[#,*]Department of Computer Science and Engineering, Panimalar Engineering College,
[#]Email: {kakshaya29, anupriyapkmsaravanan, ashwiniraj2295}@gmail.com

Abstract

Emergency scenarios are very common in healthcare domain. These situations are very unpredictable and difficult to estimate the loss and amount of injuries or diseases that could occur. Hence it is impossible for the automated systems to detect these emergency situations and cannot provide the new information's. In case of elderly persons and patients who reside at home, need to check their healthcare record periodically using the systems. At times this becomes time consuming and inefficient to use and it could also happen that the person may forget to record or monitor the values periodically. Another scenario to be considered is when the patient is alone and not able to communicate the emergency situation to the family members and doctors. Hence to help and identify this situation we propose a flexible access control framework using Complex Event Processing (CEP) technology. When an emergency is detected the temporary access control policies (tacps) will be activated. These control policies will override the regular policies in emergency cases.

Keywords: CEP, TACP, Emergency Detection, Data Sharing

INTRODUCTION

Sharing the information during emergency situations is a challenge to be tackled efficiently. Lack of sharing information could lead to inefficient and no emergency management that leads to loss of lives. For information to be shared rightly without information leakage we have modeled a ready to link access control policies and these are called as emergency policies.

The active rules based complex event process helps in monitoring patient's important values in real time scenarios. Active rules in ACEP help querying in real time scenario with real time actions. Hence the challenge is to handle the queries and the corresponding reactions in a high-volume stream execution environment. When an emergency is declared, temporary access control policies (tacps) are activated for the tasks of emergency case to be handled. Tacps will override the normal regular policies in emergency situation. Hence this is supported by regulations and laws and also risk assessment section. Based on all the above the emergency policy will be considered in place.

During situations of catastrophic events like difficulty in breathing, heart attack, stroke, loss of consciousness the proposed system will trigger emergency management. In order to efficiently share information during emergency situation we have used a flexible access control framework using Complex Event Processing technology. This helps in predicting these emergency situations. Once an emergency situation is detected the

temporary access control policies are activated and override the regular policies.

Hence the first responder to this emergency alert will be provided with the access to the information. In healthcare domain it is hard to identify the emergency scenarios and trigger an alert for the same. It is difficult to point the disease or injury that could lead to emergency and these situations are not recorded in the system because it is not prepared for such scenarios and could lead to death. Hence we have proposed Complex Event Processing (CEP) system that helps in information sharing in critical situations.

RELATED WORK

Nabil R. Adam et al proposed a method of information sharing to support situation awareness and response at the strategic level. The proposed system collects data from several autonomous systems using context-sensitive parameters to integrate, filter and understand the necessary information. The major concern with this method is information sharing through secure communication mode [1].

DAVID F. FERRAIOLO et al, invented standard for role-based access control (RBAC). Though RBAC was a successful method among various large-scale authorization managements and has received broad support but it failed to exist today as there is no-single authoritative definition that is alive now. Hence it is not widely accepted as it creates chaos and instability while using RBAC. But RBAC can be used to unify ideas and can serve as a foundation for product development, procurement and evaluation. RBAC's features and mechanism can also be used to enhance the need of the customers with its fundamental and stable set of mechanisms. This paper does not explain on the standardization of the existing model and the RBAC system but instead it enhances the RBAC components. This is designed and introduced in the RBAC system and Administrative Functional Specification [2].

Jana Bauckmann et al, implements SPIDER algorithm (Single Pass Inclusion Dependency Recognition) for detection of inclusion dependencies. In order to detect the IND all pairs of attributes must be tested.

SPIDER helps to handle this task very efficiently by testing all the attributes parallel. It can analyze 2 GB database in 20 minutes and 21 GB in 4 hours [3]

Maayan Gafny et al, proposed a detection method to identify suspicious users in the database through an application. The malicious activity is detected when the result-sets are sent to the user with respect to the request that the user sent. By analyzing the result set and the context we find a "level of abnormality". If the resulting level is above the defined threshold then an alert is sent to the security officer. Data linkage techniques are also used to link contextual features and the result-sets. In order to generate a behavioural model, Machine Learning algorithm is implemented to capture the behaviour of the system. It captures the behaviour of the legal user and the malicious user using the result-sets. The simulation was proposed to evaluate sanitized data in detecting data misuse [4].

Claudio A. Ardagna et al, provides solution for the access control issue in healthcare domain. The proposed method is based on different policy spaces, language and composition algebra. It helps in regulating rigorous nature of traditional access control systems with the "delivery of care comes first" principle [5].

Zhang Wei et al, studies on the knowledge management during natural disaster using the literature survey method. He mainly focuses on two studies in this paper namely: Wenchuan's earthquake in 2008 and Haiti's earthquake in 2010. Social media in knowledge management

during natural disaster response is analyzed using widespread of subject, knowledge timeliness, efficiently of knowledge sharing, etc. Secondly, social media's response mechanism in knowledge management in disaster cases was studied. Finally, the response of knowledge management towards disaster situation was studied. The author designed a systematic framework of knowledge management based on social media's knowledge management was built.
This includes knowledge module, user module, and function module and operation process of the system [6].

Daniela Pohl et al, uses metdata derived from videos and images that are in turn collected from Youtube, Flickr, etc in order to extract crisis sub-events. The author analyses the compatibility of using clustering concept to detect sub-events. The results of the proposed technique show high potential results. Further a survey was conducted among the practitioners on the idea of sub-event detection. The response result shows that using social media in combination with sub-event detection in emergency management is high and favorable [7].

Sigrid Schefer-Wenzl et al, introduces break glass approach based on RBAC model. This approach is extended to suit static (design time) and dynamic (runtime) consistency of the break-glass model. The extension was achievable to expand arbitrary process-aware information systems or process modeling languages with respect to RBAC and the corresponding break-glass policies. The simulation was performed on a library and runtime engine that supports all properties of the proposed method [8].

V.Nivedita et al, proposes a framework control model called the Access control model that constrains the controlled information sharing in emergency situations where the information will not be deviated from the controlled path. It also provides secure information sharing from source to destination even in case of natural calamities. Administration policies are also introduced to maintain model flexibility during emergency cases. The access control method ensures that the users verify the received information and also to detect if the information is normal or crucial and based on that it will handle the situation [9].

Eamonn Keogh et al, introduces a method to identify the time series discords. Time series discords are the subsequence of the longer time series. This time series is different from the rest of the time series subsequence and it captures the most unusual subsequence within the given time series. Time series discords can be used for improving the quality of clustering, data mining, data cleaning, anomaly detection and summarization. Discords need only one intuitive parameter that is the length of the subsequence that is different from the anomaly detection algorithm which needs more than one parameter [10].

Basic Idea of Proposed Methodology

The proposed method has Access control model for constraining controlled information sharing in case of emergency. There is a requirement of having a more robust, trustful method for information sharing during emergency situations. In case of emergency there is a need to access the patient information for which access is restricted during normal operations. Hence customized operations must be performed during emergency cases. Therefore, the essential access controls with full security guaranteed is required with no interference or jamming to make sure that the information is sent to the correct destination at the right time.

Emergency Policy Correctness

The main purpose of having emergency policy correctness in place is to have constraint the

DOI: 10.18535/ijecs/v6i3.52

temporary access control policies. There are two steps involved:

- The erasure or making of the emergency instances.
- Building/deleting the corresponding tacps (temporary access control policies).

Emergency policy correctness works even before the Emergency Handler. There are two steps involved in Emergency handler and the first step is the emergency repository that checks emergency related issues if any. Then a new emergency instance is created and the second step is tacp template repository that checks the templates involved in activated emergency if any. Now the corresponding tacp instance is created.

PROPOSED METHOD

In this method a Temporary Access Control Policy (TACP) policy is used for detecting emergency situation. Complex Event Processing server (CEP) is used for monitoring the patient health condition regularly. CEP also detects abnormal activity in the patient like heart rate, temperature, etc using wearable devices. An event will be generated on analyzing the values of the patient and if required an emergency situation will be declared. The proposed system can also detect lung cancer using symptoms tree traversal technique.

CEP Server

During emergency cases the concerned patient details are maintained separately in the CEP server. Using the unique login credentials of the patient you can login to the application and observe the values of the patient. Once the sensor detects emergency situation the type of emergency and the policy type will be decided. The policy details are maintained using xml.

TACP

When the sensors detect the emergency situation, the abnormal values are sent to the TACP (temporary access control policy). Based on the abnormal values, TACP will decide the type of policy to be assigned and the doctor to be chosen for the case. The read/write access is provided to the doctor based on TACP. The administrator will have the complete access to view patient complete details and emergency policies assigned to each patient.

Emergency Mobile Application

Once emergency is declared by the temporary access control policies, the emergency policy details of the patient and the abnormal values are sent to the doctor via SMS and also to patient relatives.

Once the SMS is received by the doctor the concerned patient's medical details are displayed in the application. After analyzing the details thoroughly, doctor will prescribe the required medicines through SMS to patient relative.

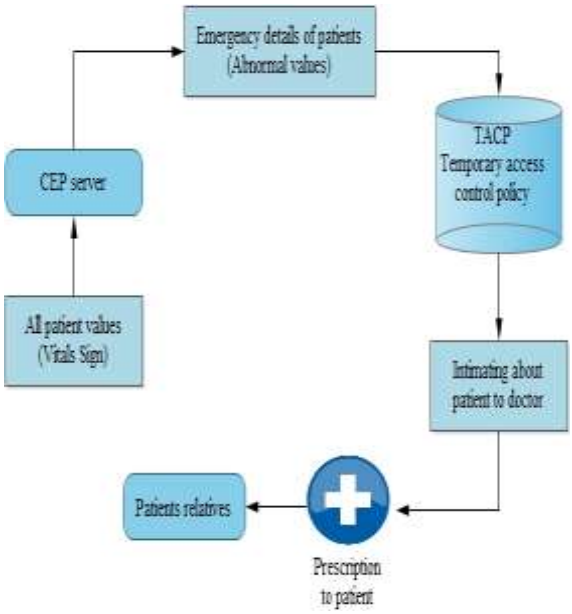

Fig 1.Block Diagram

Experimental Setup

Let's consider the picture of a patient being monitored using the emergency management system. The important values of the patient are observed and calculated using a sensor device like bluetooth. The sensor application used in this process is called the healthcare management

DOI: 10.18535/ijecs/v6i3.52

application. The vital values of the patient are recorded using Active rule based complex event processing.

Active Rule based event Processing helps in recording real time detection of abnormal events using patient's values and signs. Active rule Complex Event Processing provides efficient processing also helps in real time processing of queries and monitors events recorded through the sensors. When emergency is declared the emergency policies takes charge of temporary access control policies and helps in supporting obligations.

The temporary access control analyzer will trigger an emergency management once emergency is declared by the sensor.

Then TACP will observe the patient details and will send it to the patient's relatives and doctor using emergency management application.

Result

Fig.2.Cep server

Fig.3.Temporary access policy

Fig.4.Emergency detection

Fig.4.Emergency detection

Conclusion

The purpose of this research is to identify emergency scenarios of an abnormal person using wearable devices. When an emergency is detected the details of the patient, abnormal values are sent to the doctor and the required prescription is sent to the relatives of the patient through SMS. Hence a Mobile Application is created to notify the doctor and the relatives of the patient about the emergency situation. We have also implemented XML Based Temporary Access Control Policy (TACP) for detection of emergency situations.

REFERENCES

[1] Nabil R. Adam , Vijay Atluri , Soon Ae Chun , John Ellenberger , Basit Shafiq , Jaideep Vaidya & Hui Xiong , "Secure Information Sharing and Analysis for Effective Emergency Management", January 2008.

[2] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn And Ramaswamy Chandramouli, "Proposed NIST Standard for Role-Based Access Control", ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001, Pages 224–274.

[3] Jana Bauckmann, Ulf Leser, Felix Naumann, Veronique Tietz , "Efficiently Detecting Inclusion Dependencies",2007.

[4] Maayan Gafny, Asaf Shabtai, Lior Rokach, Yuval Elovici "Detecting Data Misuse by Applying Context-Based Data Linkage" Copyright 2010 ACM 978-1-4503-0092-6/10/10...$10.00 ,October 8, 2010.

[5] Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Sara Foresti, Tyrone W. Grandison, Sushil Jajodia, Pierangela Samarati, "Access Control for Smarter Healthcare Using Policy Spaces", July 12, 2010.

[6] Zhang Wei, Zhang Qingpu, Shan Wei, Wang Lei, "Role of Social Media In Knowledge Management During Natural Disaster Management", Volume4, Number4, issue4.34, March 2012.

[7] Daniela Pohl, Abdelhamid Bouchachia, Hermann Hellwagner ," Supporting Crisis Management via Detection of Sub-Events in Social Networks",2012.

[8] Sigrid Schefer-Wenzl, Mark Strembeck, "Generic Support for RBAC Break-Glass Policies in Process-Aware Information Systems", Copyright 2013 ACM 978-1-4503-1656-9/13/03 ...$10.00.

[9] V.Nivedita, K.Sathya, P.Manjula , "A System for Timely and Controlled Information Sharing in Emergency Situations", Vol. 2 Issue 1 Jan-March 2014.

[10] Eamonn Keogh , Jessica Lin , Ada Fu "HOT SAX: Efficiently Finding the Most Unusual Time Series Subsequence", 1550-4786/05 $20.00 © 2005 IEEE.

[11] 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.

[12] 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.

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

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

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