ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, Febuary 2016

A Survey on Secured Information Sharing

Dr. M. Senthil Kumar, M. Sumithra

Associate Professor, Dept. of C.S.E, Valliammai Engineering College,Chennai,India

P.G. Scholar, Dept. of C.S.E, Valliammai Engineering College,Chennai,India

ABSTRACT: Information privacy and security are the issues which affect emergency management system.In Automated emergency management information systems can be stolen and misused by malicious users. In order to provide secure information sharing we have investigated various policies. In this paper, we discussed about various types of access control policies which helps us to prevent data from misuse. Access control policies such as break the glass, Role based are discussed. An attribute based encryption can be used to prevent privacy by means of private key cryptography. Near field communication (NFC) technology is investigated which provide information sharing during more critical situations.

KEYWORDS: access control policies; privacy; security; emergency management; information sharing; encryption; near field technology

I. INTRODUCTION

Emergency management deals with strategic organizational management process. Many industries lacks information sharing during critical situations. Our aim is to provide technically for secure information sharing. In this paper, we have investigated secured and controlled information sharing with various domains. Firstly, we discussed about various types of event detection method for identifying changes in the state such as human, system, etc., Detection of event is possible by means of various methods such as complex event processing in [1], [2], [3] anomaly detection in [6]. Complex event processing provides an effective way of pattern matching. Complex Event processing is a framework which performs tracking and analyzing (processing) of information (data) streams of complex events.

Complex event processing (CEP) is event processing that combines information from multiple sources for patterns that suggest more complicated circumstances in [4], [5]. The main aim of complex event processing is to identify meaningful events(like change in state) and respond to them as quickly as possible. Complex event processing can be extended into active rule complex event processing and distributed complex event processing (INDCEP) in [18]. Active Complex event processing [15] is an embedded version of complex event processing engine with active roles. Active rule complex event processing provides fine grained and more efficient rule processing in real time opportunity. Whereas distributed complex event processing uses event processing in distributed networks. In network distributed complex event processing performs event processing by pushing complex event processing into a network node.

Anomaly detection is used for detecting abnormal events that occur during data stream processing. Anomaly detection makes use of two approaches, namely Knowledge based and data driven based approach Knowledge based approach includes a set of rules, policies and templates which represents predefined patterns in the information streams for the detection of anomalous behavior. Data driven approach uses a sliding time window for which the distribution of the observed data is determined.

Access to the resources for information sharing is controlled by the use of access control mechanisms. Traditional access control policies are static, i.e. remains unchanged. Whereas break the glass policy provides access to the data needed by breaking the rules only during emergencies. In role based access control model access to the resources is provided to the user based upon their roles. Whereas BTG-RBAC model is the integration of role based access control model and break the glass access control model. Attribute based encryption a group of receivers is defined by a combination of several descriptive attributes which is also known as attribute policy. Near field communication is also discussed in order to provide information about mobile system which provide secure information sharing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, Febuary 2016

II. DETECTION OF EVENT

When an organization acquires, changes in the state, due to some threats or events, then we need a method which able to deal with these type of changes, by analyzing and monitoring them. In this paper, we discussed about various method and techniques which deals with different types of events.

A. Complex Event Processing

Complex Event processing performs tracking and analyzing (processing) of information (data) streams of complex events. Complex event processing (CEP) is event processing that combines information from multiple sources for patterns that suggest more complicated circumstances. The main aim of complex event processing is to identify meaningful events (like change in state) and respond to them as quickly as possible. These events (change of state) may be happening in a single organization or among various organizations and its layers. I. e. Complex event processing in fig 1 is a framework that collects information from various events or sources. Complex event processing can be classified as two types, namely Aggregation oriented CEP and Detection oriented CEP.

- Aggregation oriented CEP executes online algorithms as soon as an event data enters the system.
- Detection Oriented CEP focuses on detecting combination of patterns or events. In our system, we make use of detection Oriented CEP.CEP also includes Hybrid approach.

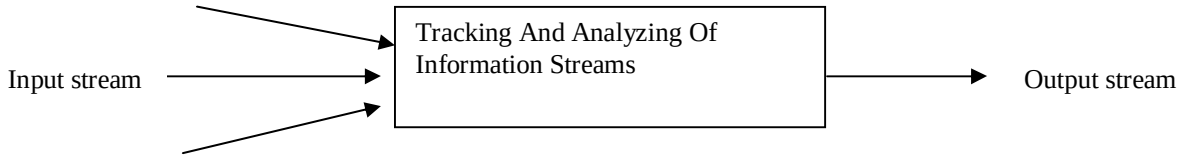

FIG 1:Complex Event Processing.

B. Active Rule Based 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. Active Rule Based CEP includes query plan and rule processing techniques. A query processing in ACEP includes the data flow pipeline of stream operators, which has SEQ, window, static-predicate, active-predicate, result construction. The SEQ engage a non deterministic finite automata (NFA) for pattern recovery. This is shown in FIG 2.

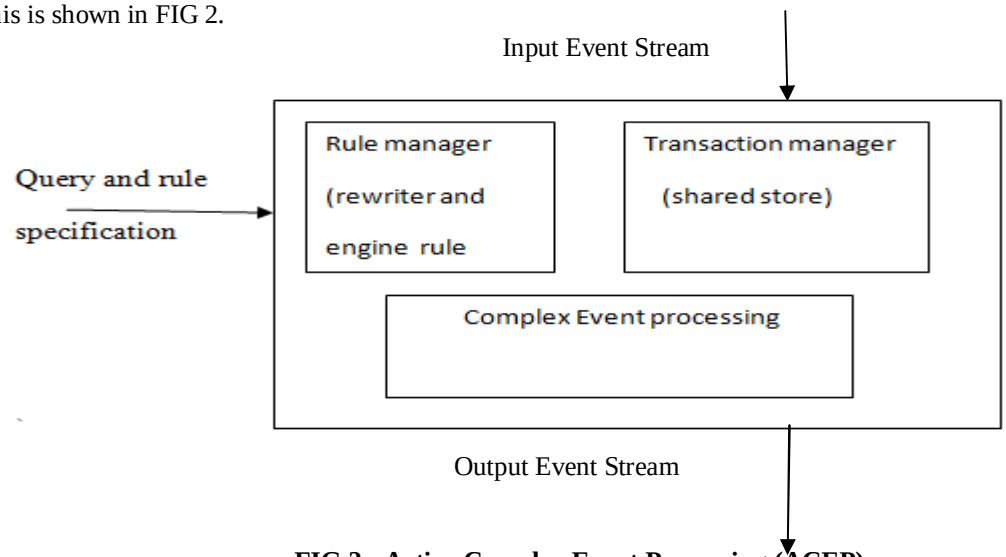

FIG 2: Active Complex Event Processing (ACEP)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, Febuary 2016

C. Distributed Based CEP

Mobile system which includes sensor network generates a unwanted event streams which can be processed efficiently by the use of In-Network Distributed Complex Event Processing(IN-CEP).INCEP [18] performs event processing by pushing complex event processing into the network nodes.this results in development of robust and high performance distributed complex event processing engine for mobile systems(CEPEMS) based on aforementioned technology.this technology performs distributed event processing by disseminating distributed plans into a network of sensor nodes to perform complex event task.It is shown in fig 3.

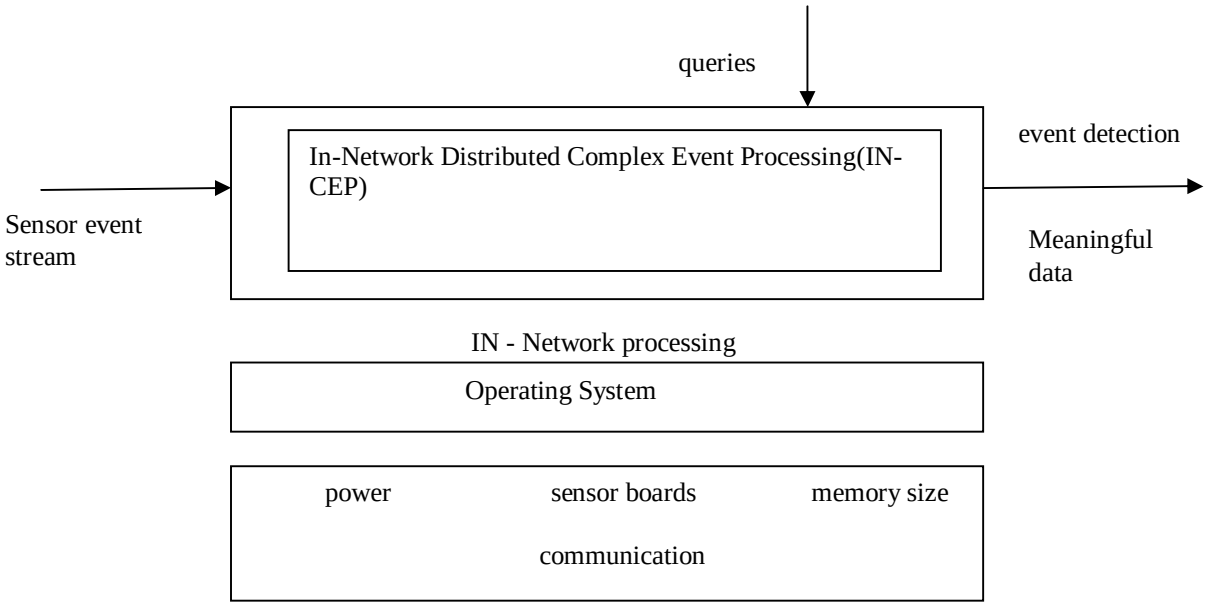

FIG 3: In-Network Distributed Complex Event Processing (IN-CEP)

D. Anomaly Detection

Anomaly detection is used for detecting abnormal events that occur during data stream processing. Anomaly detection makes use of two approaches, namely Knowledge based and data driven based approach Knowledge based approach includes a set of rules, policies and templates which represents predefined patterns in the information streams for the detection of anomalous behavior. Data driven approach uses a sliding time window for which the distribution of the observed data is determined. This distribution is compared to baseline, which provides the expected or historic behavior. The baseline is calculated using past seen data values. anomaly detection can be classified as follows: the rule-based, pattern-matching, model-based, similarity-based, and statistical approaches.

- **Rule-based approaches** use a database which contains a set of rules to determine the behavior of the faulty system(an abnormal behavior to determine whether an anomaly has occurred. The anomaly or fault is identified by monitoring a series of events that are predefined by the rules.
- **Pattern matching or profiling** make use of online learning to build profiles or patterns for normal behavior and deviation from this anomaly is determined
- **The model - based approach** uses different types of models to determine the normal behavior of the monitored system. The most popular predictive model used is unsupervised support vector machines. The model-based approaches need training data in order to build the model.
- **Parametric statistical approaches** perform model fitting and assume a known underlying distribution of the data or are based on statistical estimation of the distribution parameters. These methods flag as outliers those observations that deviate from the model assumptions. However, these methods rely heavily on prior knowledge of the data distribution and are not suitable for arbitrary or new and unknown data sets.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, Febuary 2016

III. SECURED INFORMATION SHARING

Information sharing during situations like emergency management has been investigated in various domains in order to provide efficient management strategies for incident management, planning, preparedness, etc..,Here we discuss various policies for secure sharing of data by providing access to emergency management record(object).The System [8] enables us to manage emergency situations by collecting information from different sources. Social media (Flickr and YouTube) is used to detect sub-events during an emergency situation.

A. Break the glass

Traditional access control policies are static,i.e remains unchanged. Whereas break the glass policy provides access to the data needed by breaking the rules only during emergencies.Break the glass include 3 approaches as follows,

- Pre-staging break the glass accounts: In which the access controls plan in advance in order to handle the emergency situation.
- Distributed pre-staged break the glass accounts: In this approach emergency plan for information sharing is planned and executed with help social media.
- Monitoring the use of break the glass: the use of emergency accounts needs to be monitored.

B. Role Based Access Control (RBAC)

In role based access control model access to the resources is provided to the user based upon their roles. The steps to grant access can be carried out as follows: the user sends a request for accessing object (emergency management record) to emergency management system.

- The emergency management system contacts authenticate service in order to check the whether the user authorized one.
- The authentication service returns the authentication ID for the user.
- The emergency management system calls RBAC policy analyzer passing the details about emergency, request reason, requested object.
- The RBAC analyzer returns are granted to the emergency management system (in case it is unauthorized then denied the access).
- The system performs operation and provides requested details of the user.

C. BTG-RBAC Model

BTG-RBAC model [9] is the integration of role based access control model and break the glass access control model, which includes BTG state permission in the system.Initially BTG state is set to FALSE and value changes depending upon policy rule.BTG-RBAC model is accessed by the use of check access procedure.It can hold one of three decisions, grant, deny, break the glass.

- Grant-If there is a rule granting the user's active role either the necessary permission, or permission if the BTG state is TRUE and the BTG state is actually TRUE
- Break the glass-If there is a rule granting the user's active role permission if the Btg state is TRUE but the BTG state is FALSE
- Deny-otherwise

D. Attribute Based Encryption

Attribute based encryption [7] is a public key cryptography primitive generalizing identity based encryption (IBE).In IBE a single receiver of a confidential messge is defined by a single string associated with his identity whereas in Attribute based encryption a group of receivers is defined by a combination of several descriptive attributes which is also known as attribute policy.Each user has their own descriptions such as job,status and receives related private keys

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, Febuary 2016

analogues as well.In cryptographic based operation ,attributes are directly map to a user's.i.i attribute components of the private key.

E. Near Field Communication (NFC) Technology

NFC is a short range wireless RFID technology that uses interacting electromagnetic radio fields. Electromagnetic radio fields is meant for application where physical touch is required in order to maintain security in [14].In order to use Near field Communications , the mobile phone needs to come with bundled the technology at the time of manufacture. There would be a chip inside the mobile device which contains the details of patient's information. Near field communication is the technology of the future to make payments through mobile phone devices. Besides that it can be used to pay for mobile ticketing in public transport, device acting a debit/credit card to make payments, read RFID Tag.

IV. REVIEW OF RELATED WORK

In this paper ,we discussed about various access control policies which includes regular policies, Break The Glass policy and Role Based Access Control. Detection of events using various method are also been analysed. An attribute based encryption can be used to prevent privacy by means of private key cryptography. Near field communication (NFC) technology is investigated which provide information sharing during more critical situations.

S.NO	**Title**	CONCEPT	ADVANTAGES	DISADVANTAGES
1	Controlled Information Sharing For Unspecified Emergencies	The system deals with unspecified emergencies similar to registered emergencies. Information sharing with controlled violation.	Satisfaction level measures provide efficient analysis of tap-door access control.	Alternative method for threshold calculation need to be analyzed.
2	Secure Information Sharing On Support Of Emergency Management	Detection of event that activates emergency policies. Complex event processing enables flexible information sharing.	Access control policies can be overridden during emergencies and support obligations.	Correlation analysis needs to be investigated further for more complex predicates. Alternative for emergency policy enforcement need to be analyzed.
3	A System For Timely And Controlled Information Sharing In Emergency Situations	Provide timely and flexible information sharing during emergencies. Enables access to denied access request in a controlled and temporary manner.	An extended form of administrative policy provides adjustments in the authorization.	Unspecified emergencies can't be detected. Information sharing among multiple organization is not possible.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, Febuary 2016

4	Access Control For Smarter Healthcare Using Policy Spaces	The system makes use of break the glass with the exception for restricted disclosure of date during emergency situations. Works based on 'delivery of care come first ' principle.	Policy spaces balances traditional access control system with break the glass exception.	Break the glass exception represents a back door for malicious users.
5	Detection Of Unspecified Emergencies For Controlled Information Sharing	The system deals with both specified and unspecified emergencies. A complex event processing framework provides automatic detection of unspecified emergencies.	High flexible violation for information sharing in a controlled manner.	Need to investigate more about learning techniques to automatically define new emergency policies.
6	Anomaly Detection In Information Streams Without Prior Domain Knowledge	Identify the pattern of anomalous behavior based on data driven approach. Baseline is calculated from past seen data values to determine expected or historical behavior.	Data driven approach not rely on a predefined set of rules, policies and templates.	An optimum size of the bag of words (BOW) can be calculated rather than using heuristic and domain specific values.
7	Attribute –Based Encryption With Break Glass	The System enables implementation of fine grained decentralized access control based on properties. ABE provides end to end secure information sharing.	Fast and flexible information sharing using fine grained break glass concept.	Lacks controlled override of access control policies during emergency situations.
8	Automatic Sub-Event Detection In Emergency Management Using Social Media	The System enables us to manage emergency situations by collecting information from different sources. Social media (Flickr and YouTube) is used to detect sub-events during an emergency situation.	Sub-events of large scale can be identified.	Additional data sources and streaming can be enriched.
9	How To Securely Break Into RBAC: The BTG-RBAC Model	Access to resources is provided to the user based upon their role. BTG-RBAC model allows authorized users to break the glass.	Allows users to access data in a secure and responsible way.	The BTG-RBAC model can be investigated further in order to enable exception.
10	Detecting Data Misuse By Applying Context-Based Data Linkage	Suspicious insiders who cause data misuse is identified Analysis the result-sets sent to the user following a request that sent by the user.	The Data linkage technique is used for linking the contextual features and the result sets.	To investigate more about the level of anomality.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, Febuary 2016

11	EXAM : An Environment For Access Control Policy Analysis And Management	The System supports policy property analysis, policy similarity analysis and policy integration. XACML is used for analyzing access control policies.	Management functions such as editing, storing And retrieval can be performed.	Access control policy can be analyzed further to provide flexibility in data sharing.
12	Privacy-Preserving Similarity Measurement For Access Control Policies	Asymmetric scalar product preserving encryption enables processing of nearest neighbour queries on encrypted data.	Similarity measurement in privacy preserving provides secure access of data.	Techniques for automatic mapping of categorical attribute domain need to be analyzed further.
13	Automated Healthcare Information Privacy And Security : UAE Case	Explores the importance of information sharing privacy and security in health care institutions.	Lack of information privacy and security is analyzed.	The information provided does not include full picture.
14	Mobile Healthcare System Using NFC Technology	Provides m-health care service using near field communication for providing health care systems.	NFC technology usage optimizes the cost without affecting the quality of care.	Information privacy and security is not analyzed.
15	Active Complex Event Processing Infrastructure: monitoring And Reacting To Event Streams	Active rule complex event processing technology provides fine grained and more efficient rule processing in business process.	ACEP provides improved performance in the event based processing systems.	Evaluation of rule rewriting optimization can be improved.
16	An Emergency Information Sharing (EIS) Framework For Effective Shared Situational Awareness (SSA)	The EIS provides timely incident data sharing and remotely command facility for responders. Includes distributed data sharing framework, SSA browser for information sharing at all levels of emergencies.	An EIS framework for SSA is readily achievable , cost effective ,sustainable and deployable in the near term.	Shared situational awareness can be analyzed further.
17	Distributed Complex Event Processing In Sensor Networks	In network DCEP performs event processing by pushing complex event into the network nodes. Provides efficient way of event processing in mobile systems.	INDCEP enables CEP in sensor networks to meet real time requirements and network characteristic.	Performance can be improved by further analysis of Complex event processing.
18	Secure Sharing In Distributed Information Management Applications: Problems And Directions	A hybrid code splitting and secure multi party computation provide assurances for privacy. Focuses on factors need to be considered during online information sharing .	Prevent data leakage caused by eavesdroppers ie unauthorized users who view your sensitive data.	Online data privacy is limited or complex for large scale implementation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, Febuary 2016

19	Emergency Data Awareness: Sharing Under Stress	Safety net system supports timely and comprehensive information sharing. Provides a standard mechanism for combining resource data and configured databases into a single virtual , federated network system.	Safety net supports sharing of data across multiple jurisdictions.	System needs additional features for building full production.

V. CONCLUSION AND FUTURE WORK

In this paper, we analyzed about detection of event and secure information sharing. Information privacy and security are the issues which affect emergency management system. In Automated emergency management information systems can be stolen and misused by malicious users. In order to provide secure information sharing we have investigated various policies. Complex event processing and extended versions are discussed which may be used as a monitoring unit for complex event processing in real time scenarios. In this paper, we discussed about various types of access control policies which helps us to prevent data from misuse. Thus we have explained about how making use of policies for secure and controlled information sharing during critical situations.

REFERENCES

[1] Barbara Carminati, Elena Ferrari, Michele Guglielmi, " Controlled Information Sharing For Unspecified Emergencies", International Conference on Risks and Security of Internet and Systems (CRiSIS), 2013.
[2] Barbara Carminati , Elena Ferrari, Michele Guglielmi, ,"Secure Information Sharing On Support of Emergency Management", IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing ,2011.
[3] Barbara Carminati , Elena Ferrari, Michele Guglielmi," A System For Timely And Controlled Information Sharing in Emergency Situations" ,IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 3,2013.
[4] Claudio A.Ardagna,Sabrina De Capitani Di Vimercati,SaraForesti,Tyrone W.Grandison ,"Access Control For Smarter HealthCare Using Policy Spaces", 2010.
[5] Barbara Carminati , Elena Ferrari, Michele Guglielmi ,"Detection of Unspecified Emergencies For Controlled Information Sharing",IEEE Transaction on Dependable and Secure computing, 2015.
[6] M.S. Beigi S.F.Chang,S.Ebadollahi,"Anomaly Detection In Information Streams Without Prior Domain Knowledge", 2011.
[7] AchimD.Brucker, Helmut Petritsch, Stefan G.Weber,"Attribute Based Encryption With Break Glass" ,2010.
[8] Daniela pohl, AbdelhamidBouchachia, Hermann Hellwagner ,"Automatic Sub-Event Detection In Emergency Management Using Social Media" ,2012.
[9] Ana Ferreira,DavidChadwick,PedroFarinha,Ricardo Correia ,"How to Securely Break Into RBAC:The BTG-RBAC Model", 2009.
[10] MaayanGafny,AsafShabtai,LiorRokach,Yuval Elovici,"Detecting Data Misuse By Applying Context-Based Data Linkage", 2010.
[11] PrathimaRao,Danlin,ElisaBertino,Nighuli,Jorge Lobo,"EXAM: An Environment For Access Control Policy analysis and Management,2010.
[12] Eun-Aecho,GabrielGhinita,Elisa Bertino, ,"Privacy-Preserving Similarity Measurement For Access Control Policies" ,2010.
[13] MhamedZineddine,"Automated HealthCare Information Privacy And Security:UAE case" ,International Conference Technology and security ,2011.
[14] A Devendran, Dr T Bhuvaneshwari, Arun Kumar Krishnan, , "Mobile HealthCare System Using NFC Technology", IJCSI International Journal of Computer Science Issues ,2012.
[15] Di Wang,ElkeRundensteiner,RichardT.Ellison,Han Wang ,"Active Complex Event Processing Infrastructure:Monitoring And Reacting To Event Streamas", 2011.
[16] Robert E.Balfour, "An Emergency Information Sharing(EIS) Framework For Effective Shared Situational Awareness(SSA)", 2014.
[17] PiotrMardziel,AdamBender,MichaelHicks,DaveLevin,MudhakarSrivatsa,Jonathan Katz,"Secure Sharing In Distributed Information Management Apllication:Problems And Directions" ,2010.
[18] OmranSaleh, Advisor:Kai-Uwe Sattler,"Distributed Complex Event Processing In Sensor Networks", IEEE Transactions Conference on Mobile Management ,2013.
[19] Larry Budnick,"Emergency Data Awareness:Sharing Under Stress", 2008.