ISSN:0975-9646

Kannadasan.R et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2758-2761

Reliable Communication in Event Processing Systems

Kannadasan.R
School of Computer Science and Engineering
VIT University, Vellore-632014, Tamilndu ,India

Sandeep Kumar.J
School of Computer Science and Engineering
VIT University,Vellore-632014,Tamilndu,India

Venu Kumar.B
School of Computer Science and Engineering
VIT University, Vellore-632014, Tamilndu, India

***Abstract*: Event processing is an approach that can capture and process the data about the events. Complex event processing is the merging the information from multiple origins. Event processing systems has a procedure that continuous event streams will be further applied operations of event streams. In distributed-applications like a large warehouse (where items can be shipped) when we are processing the events. This will be transmitting in between many security authorities. Using the access-policy every incoming event can be secured. We can increase the processing of events by calculating the measure of obfuscation values for events. Calculate the threshold for obfuscation as one of the part of access-policy and avoid the access-requirements and events will be delivered more reliable. In this way we can deliver the more events.**

***Keywords:* event, access-policy, security, obfuscation**.

1. INTRODUCTION:

Generally, in large business it is necessary to identify the losses early. In event processing system we take an example of shipping of items. In shipping of items are continuously tracked to identify the loss or reroute the items during the shipping. Complex event processing plays a major role in industrial and business applications [1].

Complex event processing systems [2][3] is allowed to identify the situations accordingly and operations can be performed very easily. This complex event processing systems can be performed the operations which can be emerge the sensors everywhere. In earlier, event processing systems has applied dynamic operators in central way but now event sources and consumer of events will be increased. This load will be reduced by using the distributed-network [4][5][6]. At present, in companies and groups many people are exchange the events. Events can be used in business process, weather reports, traffic reports, text messages or may be any of the event information but in complex event processing applications has no security. It is not suitable for central manage access control for whole network. Event processing networks are heterogeneous in terms of technologies or processing capabilities ,consists of different participants , are spread over multiple security-domains[7][8].

Here we are taken the event has shipping of the items perspective. For example, in a company they restrict he some data to the only legitimated users. Only the Some of the authorized company users only see the details and process the information. For example, in logistic process a manufacturer will be delivered items to the customer [4]. If at all manufacturer will delivered items to the customers it is difficult to communicate the manufacturer to the customer because there are many customers are available .sending the items to the many customers will be time consuming and if manufacturer will delivered the items to the customer if any items are missed or items quality is not good then difficult to communicate the customer to manufacturer. Deliver the items to the many customers at a time also difficult. Deliver the items through shipping company is easy process. The shipping company will ship the items before manufacturer will deliver to the customer [5].

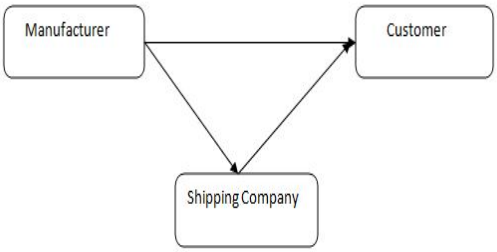

Figure 1. Access Control and Event Dependency

Shipping companies are hosted in different domains where events will exchange include the confidential information i.e. destination name, product name. In this exchange of event information third party was received the information about the event but it is confidential and given to the access rights to only the shipping company. In this event information create access-control that he secured data will be processed multiple domain in large complex event processing systems. This will allow defining the obfuscation threshold as an access policy avoids all the access restrictions and deliver the events. The number of events will be increased application will be react quickly thus the increase of complex event processing systems can be utilized.

II. RELATED WORK:

Event Processing Systems popularity is increased because of this popularity we may also consider the security of the systems. Authors Pesonen et al. and Bacon et al. they discuss how publish or subscribe systems will be secure by introduce the some of the access control policies [10],[11],[12]. They also describe how communication between events will be supported. Author Opyrchal et. al. the every event will have particular owner that will be specified. These are used to provide access to their events

[18]. Tariq et al. will propose a solution to provide confidentiality and authentications in broker less content-based publishes or subscribe systems [9]. Our work is based on the previous work which make event communication secure among different entities in the system. In event processing systems, we compute the Bayesian-inference after constructing a Bayesian-network and learning the dependencies Since Bayesian inference is a complicate computation, several Monte-Carlo algorithms have already proposed to approximate the values for inference [14]. They all have in common to randomly pick samples from the Bayesian-network probability distribution, and approximate the values based on the samples taken from the network. The precision of the inference values purely based on the number of samples. A commonly used technique is gibbs sampler [15].

III. EXISTING SYSTEM:

Earlier methods are used for measure the Bayesian-network conditional probabilities[15][16] but their accuracy may depends on the Number of patterns appropriate from the network and there is no method exists for achieve the accuracy in polynomial time. Approximate algorithms are not feasible for the security applications and no guarantee for exact time for delivery of the applications. The complication of calculate the correct inference will be decreasing the storing the partial outcome of inference computation otherwise we will compute many times. However, optimization benefits are strongly dependent on the design of Bayesian-network. Bayesian-network may be connected single connected Bayesian-network or multiple connected Bayesian-networks [1].

IV. PROPOSED SYSTEM:

In this proposed system we derive access-requirements by selecting the event attributes for access-policy. This will allows the requirements for a chain of dependent operators in G. We measure the threshold for obfuscation for attributes of events in every Correlation process obfuscation of attributes of events are produced is determined by proposed of access-policy consolidation protocol. If threshold for obfuscation is reached for any of the attribute that particular attribute Access-Requirement will be avoided.

(A). Access-policies:

Access-control will allows for specified access-rights to set of all event attributes. These Access-Rights are given by the event stream produces and gives the operators based upon Access-Requirement i.e. location or role or may be any of the event operators. Requirements are generally indirect properties for all the operators. Generally, we declare the access-rights within the Access-policy and here we declare the Access-policy as Acp for any operator ω define as set of Attributes and Access-requirements as acr .

$$Acp_{\omega} = \{(attr_1, acr1) \ldots \ldots (attr_n, acr_n)\}$$

If at all no access-requirement mentioned by default all the consumers will be access to the particular Requirement.

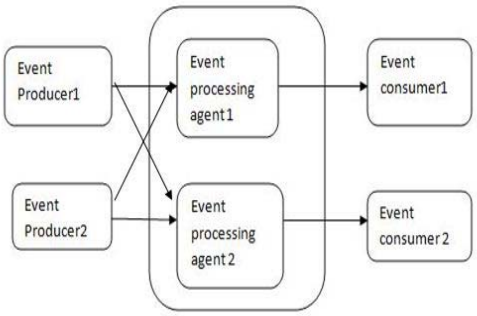

Figure 2. communication between producer and consumer

Access-Requirement is a notation it consists property p and maths operator op and a set of values is defined as acr = (p, op, Val)

In the above tuple op $\in$ *{<,>,* $\leq$ *,*$\geq$ *,*$\in$ *, =}* and val will be specified as a range of attributes.

$$Ar1 = (dom, \in, \{doma, domb\}).$$

In the above tuple only domain dom will only access the Access-requirements of doma and domb. If at all we take the manufacturer perspective this can be defined as

Acp_{manu}={(destination,(dom, $\in$,{ Shippingcompany,Consumer})), (pickup time,(dom,=,shipcompany)),(prod place,(dom,=,shipcompany))}

In the above example restrict the data about which people can access the data requirements. If at all properties of the consumer will match the Access-Requirements then only the particular consumer is access the event related information.

(B).Policy Consolidation and Event Obfuscation:

To cope up with the security goal of the above section 3 in our approach the secure event streams with the pair of the operators in the G and for the development of the secure events we have to rely on the mechanisms which are available in state of art publish systems .In our way of our approach its too important to understand the each and every customer ω_c needs to the request which is required by the event attributes and the requests which are need to handled by the producer ω_p *and* ω_c which need to authenticate itself against ω_p for the next event .After which the success of the authentication ω_p which forward to the ω_c.

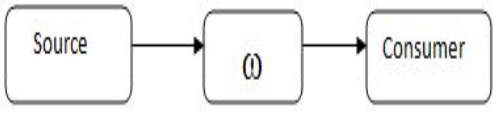

Figure 3. Single Connected correlation Network

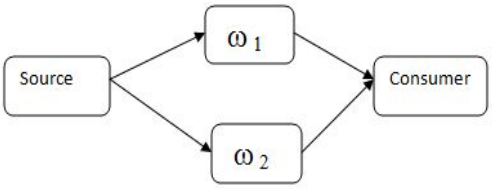

Figure 4. Multiple Connected Correlation Network

1 .The only those events which match request of the *ωc*
2. The only those events which access the policy of the attribute such that
   A. access policy of the att (attribute)allows *ωc* access *to att*
   B. attr which has achieved the sufficient high obfuscation.

(Att_i, ot_i) ∄ $OP\omega p\ obf(atti, att, \omega c) \geq oti$

To end the *ωp* with we have *to* perform the incoming streams on the acces-policy
pf the consolidation of the necessary access policies which can be inherited
and Calculated for the obfuscation values $obf(att_i, att, \omega_c)$.

V. Algorithm:

Algorithm 1: LOCAL OBFUSCATION CALCULATION
PROCEDURES initialize (ω)
  For ∀ operator ω do
    $d_\omega \leftarrow$ find multi operators(ω)
  END FOR
FOR ∄ ω ∈ d_ω Do
  Relaatts←find related Attributes
  FOR ∀ ($Attr_{new}$,$Attr_{old}$) ∈ Relatts Do
    Transmit P($Attr_{new}$/$Attr_{old}$) to ω
  END FOR
END FOR
END PROCEDURE
PROCEDURE upon receive event (e)
FOR ∄ Attr ∈ e Do
  IF MULT PATH DEPENDENCY (ATT) THEN
    Calculate Worst Case obfuscation (Att)
  ELSE
    Calculate local obfuscation (Att)
  END IF
END FOR
END PROCEDURE

(A). Scalable Access-policy Consolidation:

In Global Bayesian-Network incoming and outgoing attributes are rapidly grows. Instead of calculate the Global Network we calculate the local networks used at every host. This local network decreases the number of relations in outgoing and incoming attributes and delivers the number of events and less overhead in the network. We create local Bayesian-Network in complex event processing networks for each deployed operators. Here we are only achieve the local Bayesian-Network we are not calculate the obfuscation for many correlation steps.

(B). Measure the local obfuscation:

In this approach we compute the locally recognised dependent of attributes (i.e. $attr_{old} \rightarrow attr_{new}$) and compute the obfuscation values dependent attributes. This is having 3 advantages.

1. Graph is smaller dependent.
2. Communication-Overhead is low.
3. No multiple connected networks

In the above approach Every Host can create the Dependency-Graph locally or else we create the dependence-graph globally by using the local dependency graph we will efficiently compute the probabilities for the inference by apply variable-Elimination method.

VI. CONCLUSION:

In this paper dealt the access-policy consolidation for various complex event processing systems. The events will delivered as a multi hop process of networks so security is must for this type of networks. The proposed approach includes the algorithm that calculates the data for obfuscation this can be done in the correlation process. The value of obfuscation is used for making the decision based on the Bayesian-network. The evaluation and analysis are showing the approach is intensive of the computation. If Bayesian-Network grew processing time also increases. So we propose an approach where we calculate the local-obfuscation reach on the process of correlation. We are using variable-elimination to optimize the computing effort for obfuscation calculation.

ACKNOWLEDGEMENT

The authors would like to thank the School of Computer Science and Engineering, VIT University, for giving them the opportunity to carry out this project and also for providing them with the requisite resources and infrastructure for carrying out the research.

REFERENCES:

[1] A. Buchmann and B. Koldehofe, "Complex event processing,"*it - Information Technology*, vol. 51:5, pp. 241–242, 2009.
[2] A. Hinze, K. Sachs, and A. Buchmann, "Event-based applications and enabling technologies," in Proceedings of the Third ACM International Conference on Distributed Event-Based Systems, ser. DEBS '09. New York, NY, USA:ACM, 2009, pp. 1:1–1:15.
[3] P. Pietzuch, "Hermes: A scalable event-based middleware,"Ph.D. dissertation, University of Cambridge, 2004.
[4] G. Li and H.-A. Jacobsen, "Composite subscriptions in content-based publish/subscribe systems," in Proc of the 6th Int. Middleware Conf., 2005, pp. 249–269.
[5] G. G. Koch, B. Koldehofe, and K. Rothermel, "Cordies: expressive event correlation in distributed systems," in Proc. of the 4th ACM International Conference on Distributed Event-Based Systems (DEBS), 2010, pp. 26–37.
[6] B. Koldehofe, B. Ottenw¨alder, K. Rothermel, and U. Ramachandran, "Moving range queries in distributed complex event processing," in Proc. of the 6th ACM International Conference on Distributed Event-Based Systems (DEBS),2012, pp. 201–212.
[7] B. Schilling, B. Koldehofe, U. Pletat, and K. Rothermel, "Distributed heterogeneous event processing: Enhancing scalability and interoperability of CEP in an industrial context," in Proc. of the 4th ACM International Conference on Distributed Event-Based Systems (DEBS), 2010, pp. 150–159.

[8] B. Schilling, B. Koldehofe, and K. Rothermel, "Efficient and distributed rule placement in heavy constraint-driven event systems," in Proc. of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC), 2011, pp. 355–364.

[9] M. A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel, "Providing basic security mechanisms in broker-less publish/ subscribe systems," in Proceedings of the 4th ACM Int.Conf. on Distributed Event-Based Systems (DEBS), 2010, pp.38–49.

[10] L. I. W. Pesonen, D. M. Eyers, and J. Bacon,"Encryption-enforced access control in dynamic multidomain publish/subscribe networks," in Proc. of the 2007ACM International Conference on Distributed Event-Based Systems (DEBS), 2007, pp. 104–115.

[11] J. Bacon, D. M. Eyers, J. Singh, and P. R. Pietzuch, "Access control in publish/subscribe systems," in Proc. of the 2nd ACM International Conference on Distributed Event-Based Systems (DEBS), 2008, pp. 23–34.

[12] M. A. Tariq, B. Koldehofe, G. G. Koch, I. Khan, and K. Rothermel, "Meeting subscriber-defined QoS constraints in publish/subscribe systems," Concurrency and Computation: Practice and Experience, vol. 23, no. 17, pp. 2140–2153,2011.

[13] S. Rizou, F. D¨urr, and K. Rothermel, "Providing qos guarantees in large-scale operator networks," in High Performance Computing and Communications (HPCC), 2010 12th IEEE International Conference on, 2010, pp. 337 –345.

[14] S. J. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 2nd ed. Prentice Hall, 2002.

[15] S. Geman and D. Geman, "Stochastic relaxation, gibbs distributions, and the bayesian restoration of images," Pattern Analysis and Machine Intelligence, IEEE Transactions on,vol. PAMI-6, pp. 721 – 741, 1984.

[16] J. Shneidman, P. Pietzuch, M. Welsh, M. Seltzer, and M. Roussopoulos, "A cost-space approach to distributed query optimization in stream based overlays," in Proceedings of NetDB, 2005.

[17] Y Xing, S. Zdonik, and J.-H. Hwang, "Dynamic load distribution in the Borealis stream processor," in Proceedings of ICDE, 2005.

[18] L. Opyrchal and A. Prakash, "Secure distribution of events incontent-based publish subscribe systems," in In Proceedings of the 10th USENIX Security Symposium, 2001, pp. 281–295.