International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

Security and DependableEquivalent Service Using Fuzzy Identity-Based Encryption

Ambati Saikumar[1], Dr.Mandalapu Ekambaram Naidu Ph.D[2]

[1]PG Scholar, Dept of CSE,Arjun College Of Technology And Sciences, Hayathnagar Mandal,R.R Dist,Hyderabad,Telangana

[2]Professor, Dept of CSE,Arjun College Of Technology And Sciences, Hayathnagar Mandal,R.R Dist,Hyderabad,Telangana

ABSTRACT:

In cloud computing data centers is take a virtual servers and organization pay as the capacity of usedata centers offers and provideservices by use of virtualization techniques. Computer network storage are the principle offering of information transfers. The context of publish/subscribe is only authenticated publisher are allowed to disseminate events in the cloud and only those events is delivered to authorized subscribers. Fuzzy Identity-Based Encryption (FIBE) scheme is proposed for secure publisher/subscriber data destitution in cloud servers. FIBE uses Advanced Encryption standard (AES) is based on Symmetric Key Algorithm.We present a contentbased publish/subscribe function is routed over a peer-to-peer network model. The implications of combining methods is explored and a particular implementation. We exploit hierarchical key derivation algorithms to encode publication-subscription matching semantics for scalable key management and develop a probabilistic number of event routing algorithm to minimize the small information that can be inferred by the routing nodes. An experimental evaluation of our prototype model the PS Guard meets the security requirements while modify the performance and security of a pub-sub network.

Index Terms: Publish/subscribe, content-based routing, peer-to-peer networks, graph topology, Fuzzy Identity Based Encryption, Public key generator.

1. INTRODUCTION

Cloud computing is an emerging computing environment that enables users to store their data remotely into a cloud to enjoy scalable services on-demand. Cloud security refers to a broad set of access control policies developed for data protection [1]. The publish/subscribe framework is an efficient application for interconnecting the data sharing in a distributed environment. Publish/Subscribe systems [2] contain information providers who publish events to the system and information consumers subscribe to particular categories of events within the system by issuing subscriptions. The system ensures the timely delivery of published events to all interested subscribers. There are two general categories of publish/subscribe systems which are subject-based and content-based. In subject-based systems, the event belongs to one of a fixed set of subjects based on the attributes [3]. Network virtualization in cloud computing environment brings out reliable advantages. It can be implemented at various protocol layers, virtual private network, and Virtual Local Area Network (VLAN) and overlay network [4]. Overlay network is a network that is organizes on any other non-logical network. Nodes in the overlay network can be view as being interconnected by logical links, which corresponds to a path, possibly through many physical links, in the elementary network. This paper analyzed different routing algorithm such as Distributed Hash Table routing[3], Key Based Routing, content based routing that will be analyses in the virtualized network for efficient routing to improve the lookup of data and latency. Here location of data can be considered as metric to search a nearby data available. DHT from theory to practice and solve many practical problems such as load balance, multiple replicas, consistency, latency and soon [5]. It is implemented in two types of entities such as router and services. Harvester technique content of messages can be store as a formatted message, used intermediate between the client and router. It is applicable in mail transfer agent stores, news server, legacy system and databases. The problem in this technique is that complete content of message consists of header and body, in body section long part cannot be examined in the process of routing [6].

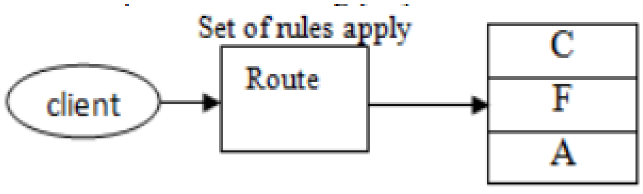


Fig no 1. The Process of Routing

2. RELATED WORK

Cipher Policy Attribute-Based Conversion (CP-ABC) [7], provides the construction of a cipher text, where a user's private key will be associated with an arbitrary number of attributes expressed as strings. It uses monotonic access trees with the help of gates to perform the complex operations. In Key-Policy Attribute Based Encryption [8], cipher texts are associated with sets of functional attributes, and keys of user containing with detailed policies. The user has no control over the accessing permissions or the authorization of users. A third party is trusted for issuing the key based on the intelligence for the process of key generation. CP-ABE has no control over the user privileges. A Semantic Overlay is a novel design principle for reliable content-based publish/subscribe architectures with self capabilities. A Distributed Publish/Subscribe (DPS) system [9] is not based on a network of brokers. Subscriber co-ordinate among themselves on a peer-to-peer basis to construct an optimized event diffusion path without any human intervention. A subscription-driven semantic overlay [9] is proposed where subscribers self organize according to similarity relationships based among their subscriptions. Groups of subscribers self-configure to form tree structures such that only one tree is built per attribute. The mapping of DHT-based overlay is not needed in typical publish/subscribe system and all types of attributes and constraints can be directly supported. Cloud computing is widely used in distributed and mobile computing environment [10]. The significance of the routing is considered as an important part in the cloud computing since they are based on the on–demand networks. Hence allocating the nearest data is a vital role in cloud computing. Data centres are the essential parts of cloud computing. In a single data centre generally thousand of virtual servers [11] run at any instance of time, hosting many tasks and at the same time the cloud system keeps receiving the batches of task requests. Traditional approach that are used in routing cannot be well in managing nodes and it is affected by network latency and inability to reach the specified location However in cloud, it is tolerable to find near best solution for routing problem in cloud environment[12]. Our earlier work focused on guarding a pub-sub network from denial of service (DoS) attacks and hard proposed several techniques to safeguard a pub-sub network against message spoofing, spamming, and flooding attacks, addressing the issue of maintaining authentication and availability of publications and subscriptions. In contrast, PSGuard presented in this paper focuses solely on secure content-based event disseminatin using a semihonest pub-sub network. Our ongoing research is to develop a secure pub-sub infrastructure that integrates with PSGuard.

3. Threat Model

We assume an honest-but-curious model for the publishers, the subscribers and the routing nodes. A curious publisher may be interested in reading the events published by other publishers. For subscribers, authorization is defined on a per subscription basis and is valid within a one subscription epoch. A subscriber S is authorized to read an event e if the event e matches one of its active subscription filters. We assume that a subscriber S who is authorized to read an event e does not reveal its contents to other unauthorized subscribers unauthorized subscribers may be curious to read those events that do not match their subscriptions [13]. Curious routing nodes in the pub-sub network may eavesdrop on the pub-sub messages routed through them. However, we assume that the pub-sub nodes are honest in routing messages from publishers to subscribers. For instance, we do not consider message dropping or malicous message forwarding based denial of service attacks in this paper, although these issues can be handled using solutions that are orthogonal to our proposal. Finally, we assume that the underlying IP-network may not offer any confidentiality or integrity guarantees.

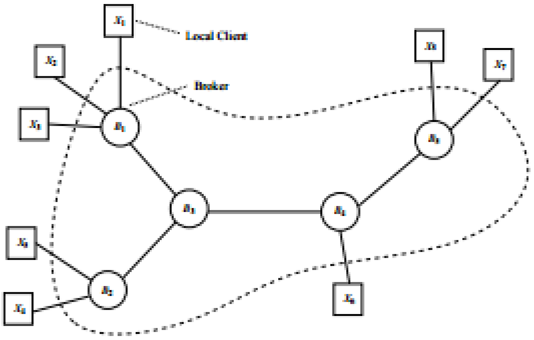


Figure 2: The router network of Rebecca.

HTS introduces an additional layer of abstraction above the standard Hermes middleware to provide an integrated view of transaction and event notification services for transactional application development. The different HTS components at the publisher and subscriber-side are depicted. The deployment of these components. The purpose of the transaction service's API is to allow the publication and consumption processes of events to be demarcated within a transaction. In general, developers implementing publish/subscribe applications that handle specific event types need the definition of these event types at development time. The use of transactions also requires that event types published as part of a transaction are known. The definition of a transaction then includes: 1) the definition of a census event type TxType used to advertise the transaction and 2) the definition of each event type evType published in the transaction. With the proposed API, publishers explicitly demarcate the scope of transactions that are advertised via census events. On receipt of a census event, a subscriber can decide whether to join a transaction; in which case, the consumption process for any received events within the transaction is implicitly considered as part of the transaction.

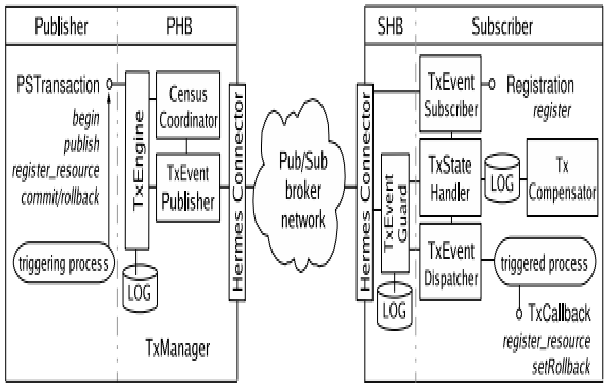


Figure 3. HTS architecture

As part of the transaction, the publisher can publish one or more events of the same or different type evType using publish and register local resources (e.g. databases), via register resource. Depending on the application scenario, events published in the transaction could just extend the information conveyed in the census event or provide a basis for structuring interrelated data Finally, a publisher requests the transaction manager to commit or abort a transaction using commit or abort. The transaction service at the client-side can be seen as an interposed coordinator between a local resource used by a client and the transaction manager[14] . Instead of having every resource directly involved with the transaction manager, at each client the transaction service merely collects votes from locally involved resources and passes a general decision to the transaction manager, which then decides on the overall outcome of the transaction.

4. PROPOSED METHODOLOGY

In the proposed system we implemented the Fuzzy technique which provides high security for data transmission. Fuzzy Identity Based Encryption (FIBE) [15] scheme is proposed for secure publish/subscribe based data sharing in cloud servers. The FIBE scheme is able to efficiently achieve a flexible access control by separating the access control policy into two parts:

i. A set of recipient identity set

ii. An access control policy derived from an attribute.

Using the FIBE scheme, a user can encrypt data by specifying a recipient ID set an access control policy over attributes, so that only the user whose ID belonging to the ID set or attributes satisfying the access control policy can decrypt the corresponding data

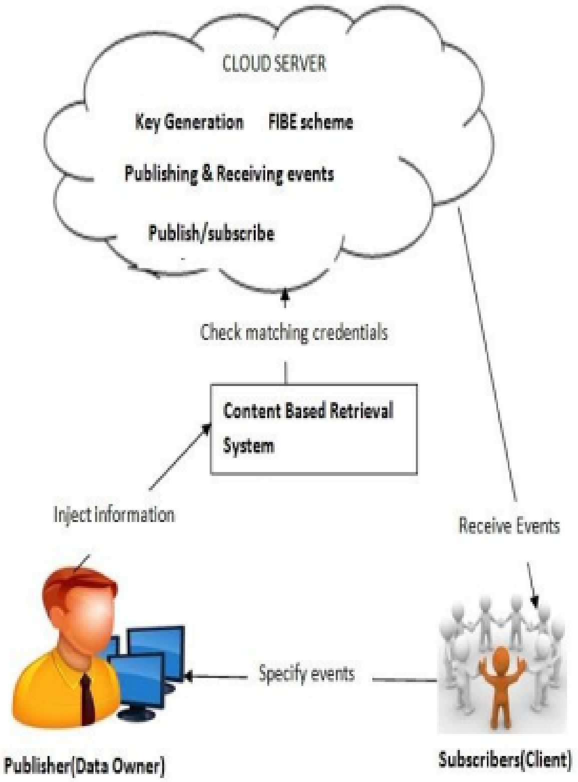


Fig.4. Architecture of Fuzzy attribute publish/subscribe system

The fuzzy is composed of a set of attributes which are classified with the events among their matching of credentials. . The attributes are based on the process of their range, id, domain of subscription, etc.., which cannot be identified based on the assumption. Each of their functions is based along the matching of credentials that is generated according to a particular scheme.

5. SECURE OVERLAY PROTOCOL

In Secure Overlay algorithm [16], the procedure to decrypt the request is done by decrypting one of the cipher texts in the connection request message.

Secure overlay dissemination protocol at peer sq.

```
Upon event Receive (ER of snew from sp) do
if decrypt request(ER)== SUCCESS then
if degree(sq) == available then
//can have child peers
Else
forward ER to child peers and parentg _ sp
if decrypt request(ER)== FAIL
then
```

ifsp == parent

then

Try to swap by sending its own ER to the snew.

Else

Forward to parent

Symmetric key encryption [17] is a public key encryption that uses the same public and private key. The master key is generated by the cloud server based on the matching of credentials that are associated with the user attributes. Symmetric Encryption is used to encrypt large amount of data without any load limits. Advanced Encryption standard (AES) is used for large data transmission beyond the size of subscription. The key size is generated randomly based on the pseudorandom generators to avoid assumption of key.

Tapestry:

Tapestry [18] is a peer to peer overlay routing infrastructure, helps in offering location-Independent, scalable and efficient routing of messages using only local resources. Each node maintains its routing table which consists of set of neighbouring nodes. When a node routes an incoming message, the node selects the next hop node from the neighbours by matching the level prefix which is similar to the longest prefix routing method. As a result the ID"s of the node on a route vary gradually119]. Unstructured overlay network: Unstructured is a decentralization approach and it"s not distributed system. Some of the protocols used in this network such as free net, Gnutella, Fast Track, Bit Torrent, Over Net/eDonkey.These methods are inefficient between topology and data location lookup .

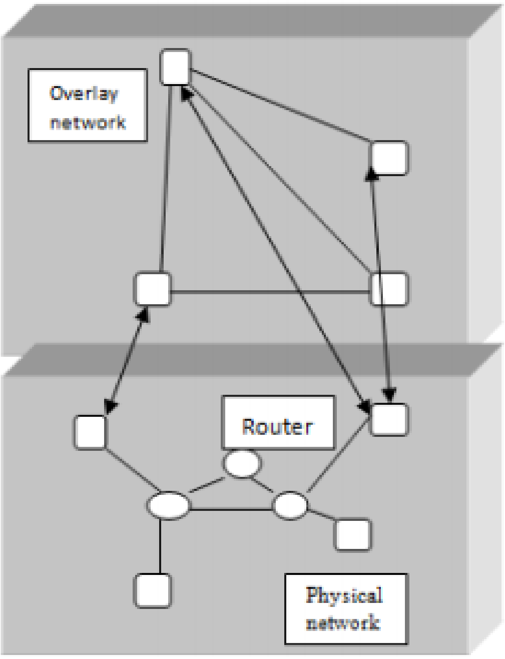


Figure 5 Structure of Overlay Network

6. PERFORMANCE CONSIDERATION

In Cloud Computing performance can be evaluated based on the parameter and its characteristics and there are different performance consideration [20] criteria for cloud infrastructure, such as

- Compute
- Storage
- Network
- Security and access
- Service offerings
- Support and service level agreements
- Managements and DevOps

The main challenges [20] for the large enterprises are given below:

- Availability: Cloud services should Be available for both providers and user.
- Storage: the performance can be degrade based on disk capacity and buffered capacity, if the request rejected by the server one of the criteria can degrade.
- Fault tolerance: In case of failure occur in datacenter ,should provide an minimum services
- Recovery: It should increase the performance based on the time that take less to recover otherwise performance will degrade.
- Routing: Location is the main factors for the network performance, the data retrieval from various data center cannot know.
- Security: Attacks on the cloud services may cause an issue on security

In propose work considering different routing algorithm for efficient network transparency and easy lookup the data from various data centers. Implement the network virtualization by considering all the resources as virtual and make deploy in cloud stack environment

7. CONCLUSION

We presented a content-based publish/subscribe system built on top of a dynamic peer-to-peer overlay network. It distributes load equally by maintaining independent delivery trees for each node. A P/S transaction demarcates, within an atomic unit-of-work, the production, delivery, and processing of a number of related asynchronous event notifications. The service is in charge of enforcing the required dependencies between the transactional contexts of interacting components and ensuring the atomicity of operations.we implemented Fuzzy Identity Based Encryption (FIBE) scheme. FIBE approach is highly scalable in terms of number of subscribers in the system and the number of limited keys maintained by them. FIBE allows subscribers to verify the authenticity of events where only an authorized subscriber can decrypt the event based on the attribute based cryptographic mechanisms and bilinear mapping A secure overlay maintenance protocol proposed for event dissemination strategies to preserve the weak subscription confidentiality. FIBE enables secure message sharing between the publisher and subscribers based on attributes.

8. FUTURE WORK

While we do not assume any specific filter model to be implemented on top of our infrastructure, there are a number of general constraints on content-based filter models as described .In addition to these, our system favours filter models that allow to limit the size of update messages between the nodes. It remains to be seen what filter models can actually be implemented efficiently on top of our architecture. It is an interesting challenge to investigate the impact of physical locality on the behaviour of publishes or subscribe. We expect that there are trade-offs to be made in choosing which edges connect physically proximate nodes.

9. REFERENCES

[1] Dataperminite. (2014). [Online]. Available: http://www.domo.com/blog/2012/06/how-much-data-is-created-every-minute/

[2] TariqM.A, and Rothermel.K, Valtaweel.A, (2010),"Providing Basic Security Mechanism in Broker-Less Publish/Subscribe Systems," Proc. ACM Fourth Int'l Conf. Distributed Event-Based Systems (DEBS)

[3] Khan. I. Koch, Koldehofe.B, Rothermel.K,(2011)"Meeting Subscriber-Defined QoS Constraints in Publish/Subscribe Systems," Concurrency and Computation: Practice and Experience, vol. 23.

[4] Franco Callegati,WalterCerroni, Chiara Contoli:performance of multi-tenant Virtual Networks in Open stackbased Cloud Infrastructures, IEEE transactions on cloud computing in 2013.

[5] Hao Zhang, Yonggang Wen, HaiyongXie, and Nenghai Yu: A Survey on Distributed Hash Table (DHT): Theory,

Platforms, and Applications "survey paper „July 2013.

[6] HariBalakrishnan, M. FransKaashoek, David Karger, Robert Morris, Ion Stoica_MIT Laboratory for Computer Science" Looking Up Data In P2p Systems.

[7] Bethencourt.J,.Sahai.A, and Waters.B, "Cipher text-Policy Attribute-Based Encryption","Proc. IEEE Symp.Security and Privacy.

[8] Srivatsa.U, Liu.L, and Iyengar.A, (2011) "Event Guard: A System Architecture for Securing Publish-Subscribe Networks," ACMTrans. Computer Systems, vol. 29.

[9] Anceaume.E, Gradinariu.M, Simon.G, and Virgillito.A, "A Semantic Overlay for SelfPeer-to-Peer Publish/ Subscribe," Proc. 26th IEEE Int'l Conf. Distributed Computing Systems (ICDCS)

[10] David B. Johnson, David A. Maltz, and Yih-Chun Hu;" The Dynamic Source Routing protocol for mobile ad hoc networks (DSR). Internet draft (work in progress)", IETF, April 2003

[11] Franco Callegati,WalterCerroni, Chiara Contoli:performance of multi-tenant Virtual Networks in Open stackbased Cloud Infrastructures, IEEE transactions on cloud computing in 2013.

[12] Antony Rostrum and Peter Druschel, "Pastry: Scalable, distributed object location and routing for large –scale peer to –peer systems, in proc.IFIP/ACM middleware 2001, Jan germany , Nov 2001.

[13] G. Banavar, T. Chandra, B. Mukherjee, and J. Nagarajarao. An efficient multicast protocol for content-based publish subscribe systems. In Proceedings of the 19th ICDCS, 1999.

[14] N. Krishnakumar and A. Sheth.Managing Heterogeneous Multisystem Tasks to Support Enterprise-Wide Operations. Distributed and Parallel Databases, 3(2):155–186, 1995

[15] Khan. I. Koch, Koldehofe.B, Rothermel.K,(2011)"Meeting Subscriber-Defined QoS Constraints in Publish/Subscribe Systems," Concurrency and Computation: Practice and Experience, vol. 23

[16] TariqM.A, and Rothermel.K, Valtaweel.A, (2010),"Providing Basic Security Mechanism in Broker-Less Publish/Subscribe Systems," Proc. ACM Fourth Int'l Conf. Distributed Event-Based Systems (DEBS)

[17] Ion.M, Crispo.B, Rusello.P (2010) “Supporting Publication and Subscription Confidentiality in Publish/Subscribe Networks in Cloud,” Proc. SixthInt’l ICST Conf. Security and Privacy in Comm. Networks (Secure Comm.), vol.32.

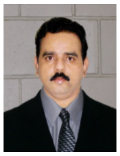
[18] KeongLua; Crow croft, Jon; Pias, Marcelo; Sharma, Ravi; Lim, Steve."IEEE Survey on overlaynetworkschemes".CiteSeerX: 10.1.1.111.4197: covering unstructured and structured decentralized overlay networks including DHTs (Chord, Pastry, Tapestry and others).

[19] Xingkong Ma, Student Member, IEEE, Yijie Wang, Member, IEEE, and Xiaoping Pei: A Scalable and Reliable Matching Service for Content-based Publish/Subscribe Systems, IEEE Transactions on Cloud Computing VOL: PP NO: 99 Year 2014.

[20] NiloofarKhanghahi and Reza Ravanmehr:” Cloud Computing Performance Evaluation: Issues and Challenges” International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.5, October 2013

Student:

Ambati Saikumar, M.Tech(CSE),Arjun College Of Technology And Sciences, Hayathnagar Mandal,R.R Dist,Hyderabad,Telangana.



Guide:

Prof.Dr.Mandalapu Ekambaram Naidu Ph.D,Computer Science,University of Mysore,Mysore ,2009.

Email:menaidu2005@yahoo.co.in