ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Methodology in Building a Scalable and Reliable Matching Service for Content Based Systems

G Kumar
Associate Professor
Department of CSE
Lords Institute of Engineering and Technologies.

Reni.T
M.Tech (CSE)
Department of CSE
Lords Institute of Engineering and Technologies.

ABSTRACT

In this paper we study about how to distribute large-scale live content to interested users in a scalable and reliable manner. How to distribute large-scale live content to interested users in a scalable and reliable manner. The publish/subscribe (pub/sub) model is widely used for data distribution because of its capacity of seamlessly expanding the system to massive size. However, most event matching services of existing pub/sub systems either lead to low matching throughput when matching a large number of skewed subscriptions, or interrupt distribution when a large number of servers fail. The cloud computing provides great opportunities for the requirements of complex computing and reliable communication. In this paper, we propose SREM, a scalable and reliable event matching service for content-based pub/sub systems in cloud computing environment. To achieve low routing latency and reliable links among servers, we propose a distributed overlay Skip Cloud to organize servers of SREM. Through a hybrid space partitioning technique HPartition, large-scale skewed subscriptions are mapped into multiple subspaces, which ensures high matching throughput and provides multiple candidate servers for each event.

INTRODUCTION

Common requirement for any system is security. The need for security must be extremely high. It is one of the major requirements to protect or control any sort of failures. There are number of mechanisms which are available to provide security. In that one of the most important mechanisms is encryption. In cryptography encryption is the process of converting plain text to cipher text which is unreadable from unauthorized users. The cryptography mechanism is required in publish/subscribe system. In publish/subscribe system publisher is one who publishes his content without specifying a particular destination to reach publisher will not program the documents to be delivered to a particular subscriber. Publisher will classify publishing documents based on different criteria and release it and subscriber will show interest on one or more documents and subscribe to that particular one in order to have access over it. This publish/subscribe system is traditionally carried out in broker-less [12] content based routing which forwards or routes the message based on the content of the message instead of clearly routing to an specified destination.

Content based routing applies some set of rules to It's content to find the users who are interested in its content. Its different nature is helpful for huge-level scattered applications and also provides a high range of flexibility and adaptability to change. Authorized publisher have permission to publish events in the network and similarly subscribers who likes the content can gets subscribed to a particular published content and have access over it by which high level

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

access control [7] can be achieved. Here published content should not be exposed to routing infrastructure and subscribers should receive content without leaking subscription identity to the system, which is a highly challenging task which needs to be carried out in content-based pub/sub system. Publisher and subscriber are the two entities and they do not trust each other. Even though authorized publisher publish events, nasty publisher pretend to be the real publisher and may spam the network with fake and duplicate contents similarly subscribers are very much eager to find other users and publishers which are challenging tasks. Finally, Transport Layer Security (TLS) or Secure Socket Layer (SSL) is secure channels for distributing keys from key server to the required. Existing security approach deals with traditional network and security is based on restricted manner which tells about key word matching [8]. Key management was the challenging task in the existing approach, so to overcome all these, we use new approach called pairing-based cryptography mechanism, which helps in mapping between to end parties so called cryptographic groups. Here, Identity Based Encryption Technique (IBE) [9] is used under this mechanism. New approach IBE provide greater concern towards authentication and confidentiality in the network. Our approach permit users to preserve credentials based on their subscriptions. Secret keys provided to the users are labeled with the credentials. In Identity-based encryption (IBE) mechanisms 1) key can be used to decrypt only if there is match between credentials with the content and the key; and 2) to permit subscribers to check the validity of received contents. Moreover, this approach helps in providing fine-grained key management, effective encryption, decryption operations and routing is carried out in the order of subscribed attributes.

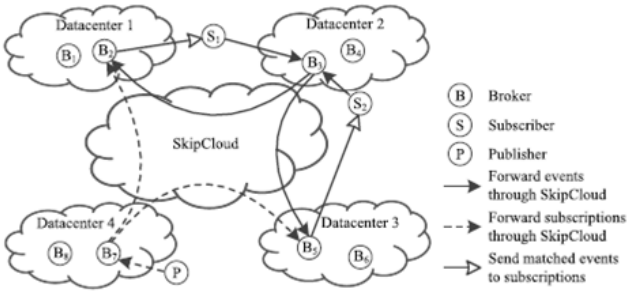
EXISTING SYSTEM:

- In traditional data dissemination applications, the live content are generated by publishers at a low speed, which makes many pub/subs adopt the multi-hop routing techniques to disseminate events.
- A large body of broker-based pub/subs forward events and subscriptions through organizing nodes into diverse distributed overlays, such as tree based design, cluster-based design and DHT-based design.

DISADVANTAGES OF EXISTING SYSTEM:

- The system cannot scalable to support the large amount of live content.
- The Multihop routing techniques in these broker-based systems lead to a low matching throughput, which is inadequate to apply to current high arrival rate of live content.
- Most of them are inappropriate to the matching of live content with high data dimensionality due to the limitation of their subscription space partitioning techniques, which bring either low matching throughput or high memory overhead.

SYSTEM ARCHITECTURE:



PROPOSED SYSTEM:

- Specifically, we mainly focus on two problems: one is how to organize servers in the cloud computing environment to achieve scalable and reliable routing. The other is how to manage subscriptions and events to achieve parallel matching among these servers.
- We propose a distributed overlay protocol, called SkipCloud, to organize servers in the cloud computing environment. SkipCloud enables subscriptions and events to be forwarded among brokers in a scalable and

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

reliable manner. Also it is easy to implement and maintain.

- To achieve scalable and reliable event matching among multiple servers, we propose a hybrid multidimensional space partitioning technique, called HPartition. It allows similar subscriptions to be divided into the same server and provides multiple candidate matching servers for each event. Moreover, it adaptively alleviates hot spots and keeps workload balance among all servers.

ADVANTAGES OF PROPOSED SYSTEM:

- We propose a scalable and reliable matching service for content-based pub/sub service in cloud computing environments, called SREM.
- We propose a hybrid multidimensional space partitioning technique, called HPartition SSPartition.
- To alleviate the hot spots whose subscriptions fall into a narrow space, we propose a subscription set partitioning,
- Through a hybrid multi-dimensional space partitioning technique, SREM reaches scalable and balanced clustering of high dimensional skewed subscriptions

MODULE DESCRIPTION:

1. Scalable and Reliable Event Matching.
2. Skip Cloud Performance.
3. Hybrid multidimensional partition Technique.
4. Publisher/Subscriber Module.

Scalable And Reliable Event Matching:

All brokers in SREM as the front-end are exposed to the Internet, and any subscriber and publisher can connect to them directly. To achieve reliable connectivity and low routing latency, these brokers are connected through an distributed overlay, called SkipCloud. The entire content space is partitioned into disjoint subspaces, each of which is managed by a number of brokers. Subscriptions and events are dispatched to the subspaces that are overlapping and events falling into the same subspace are matched on the same broker. After the matching process completes, events are broadcasted to the corresponding interested subscribers.

SkipCloud Performance:

SkipCloud organizes all brokers into levels of clusters. At the top level, brokers are organized into multiple clusters whose topologies are complete graphs. Each cluster at this level is called top cluster. It contains a leader broker which generates a unique b-ary identifier with length using a hash function cluster are responsible for the same content subspaces, which provides multiple matching candidates for each event. Since brokers in the same top cluster generate frequent communication among themselves, such as updating subscriptions and dispatching events, they are organized into a complete graph to reach each other in one hop. After the top clusters have been well organized, the clusters at the rest levels can be generated level by level.. This identifier is called ClusterID.

Hybrid multidimensional partition Technique:

Achieve scalable and reliable event matching among multiple servers; we propose a hybrid multi-dimensional space partitioning technique, called HPartition. It allows similar subscriptions to be divided into the same server and provides multiple candidate matching servers for each event. Moreover, it adaptively alleviates hot spots and keeps workload balance among all servers. HPartition divides the entire content space into disjoint subspaces. Subscriptions and events with overlapping subspaces are dispatched and matched on the same top cluster of SkipCloud. To keep workload balance among servers, HPartition divides the hot spots into multiple cold spots in an adaptive manner.

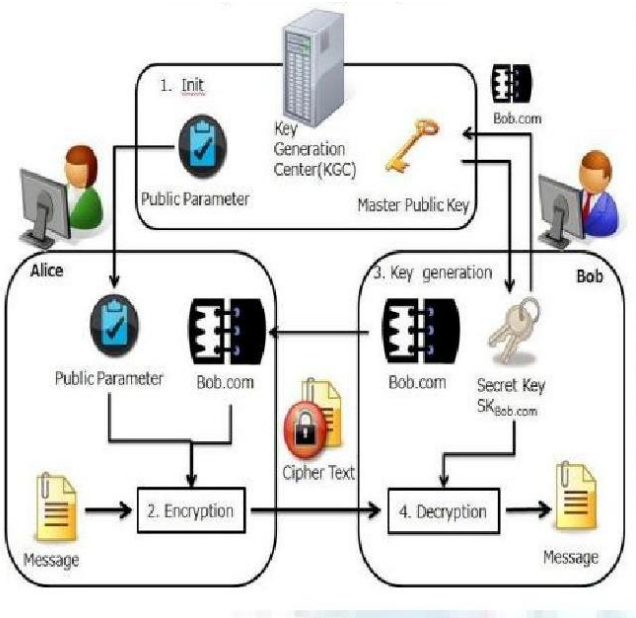
Publisher/Subscriber:

Each subscriber establishes affinity with a broker (called home broker), and periodically sends its subscription as a heartbeat message to its home broker. The home broker maintains a timer for its every

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

buffered subscription. If the broker has not received a heartbeat message from a subscriber over Tout time, the subscriber is supposed to be offline. Next, the home broker removes this subscription from its buffer and notifies the brokers containing the failed subscription to remove it.

IDENTITY BASED ENCRYPTION SYSTEM



CONCLUSION

In this paper, we have presented broker-less approach in content based publish subscribe system for providing authentication and confidentiality. The approach is extremely good for number of subscribers and publishers in the system and the number of keys maintained by them. The keys will be in cipher text format which are labeled with credentials assigned to publishers and subscribers. This paper introduces SREM, a scalable and reliable event matching service for content-based pub/sub systems in cloud computing environment. SREM connects the brokers through a distributed overlay Skip- Cloud, which ensures reliable connectivity among brokers through its multi-level clusters and brings a low routing latency through a prefix routing algorithm. Through a hybrid multi-dimensional space partitioning technique, SREM reaches scalable and balanced clustering of high dimensional skewed subscriptions, and each event is allowed to be matched on any of its candidate servers. Extensive experiments with real deployment based on a CloudStack testbed are conducted, producing results which demonstrate that SREM is effective and practical, and also presents good workload balance, scalability and reliability under various parameter settings.

REFERENCES

[1] Xingkong Ma, Student Member, IEEE, Yijie Wang, Member, IEEE, and Xiaoqiang Pei, "A Scalable and Reliable Matching Service for Content-Based Publish/Subscribe Systems" IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 3, NO. 1, JANUARY-MARCH 2015.

[2] M. Ion, G. Russello, and B. Crispo, "Supporting Publication and Subscription Confidentiality in Pub/Sub Networks," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), 2010.

[3] L.I.W. Pesonen, D.M. Eyers, and J. Bacon, "Encryption-Enforced Access Control in Dynamic Multi-Domain Publish/Subscribe Networks," Proc. ACM Int'l Conf. Distributed Event-Based Systems (DEBS), 2007.

[4] P. Pietzuch, "Hermes: A Scalable Event- Based Middleware," PhD dissertation, Univ. of Cambridge, Feb. 2004.

[5] M. Srivatsa, L. Liu, and A. Iyengar, "EventGuard: A System Architecture for Securing Publish-Subscribe Networks," ACM Trans. Computer Systems, vol. 29, article 10, 2011.

[6] A. Shikfa, M. O ¨ nen, and R. Molva, "PrivacyPreserving Content-Based Publish/Subscribe Networks," Proc. Emerging Challenges for Security, Privacy and Trust, 2009.

[7] J. Bacon, D.M. Eyers, J. Singh, and P.R. Pietzuch, "Access Control in Publish/Subscribe Systems," Proc. Second ACM Int'l Conf. Distributed Event-Based Systems (DEBS), 2008.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[8] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT), 2004.

[9] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, 2001.

[10] H. Khurana, "Scalable Security and Accounting Services for Content-Based Publish/Subscribe Systems," Proc. ACM Symp. Applied Computing, 2005.

[11] C. Raiciu and D.S. Rosenblum, "Enabling Confidentiality in Content-Based Publish/Subscribe Infrastructures," Proc. IEEE Second CreatNet Int'l Conf. Security and Privacy in Comm. Networks (SecureComm), 2006.

[12] M.A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel, "Providing Basic Security Mechanisms in Broker-Less Publish/ Subscribe Systems," Proc. ACM Fourth Int'l Conf. Distributed Eventt- Based Systems (DEBS), 2010.