SECURING LIAISON-LESS PUBLISHER/SUBSCRIBER SYSTEMS USING IDENTITY BASED ENCRYPTION

S.Kranthi[1], Madhavi Nalluri[2], Tejaswi Nadakuditi[3], Y.Shekinah[4], S.Mahesh[5]

[1]Assistant Professor, Department of Information Technology, VRSEC, Vijayawada, India
[2,3,4,5] V.R Siddhartha Engineering College, Department of Information Technology, Vijayawada, India

---***---

Abstract - *The provisioning of fundamental security components, for example, authentication and confidentiality is extremely challenging in a content based publish/subscribe framework. Verification of publishers and subscribers is hard to accomplish because of the free coupling of publishers and subscribers. Moreover, confidentiality of events and subscriptions clashes with content based routing. This paper displays a novel approach to deal with confidentiality and authentication in a liaison less content based publish/subscribe system. The verification of publishers and subscribers and secrecy of events is guaranteed, by adapting the pairing based cryptography mechanisms, to the necessities of a publish/subscribe system. Moreover, an algorithm to bunch subscribers as indicated by their subscriptions protects a weak notion of subscription confidentiality. Moreover to our past work this paper contributes 1) utilization of searchable encryption to enable effective directing of encrypted events, 2) multicredential steering another event distribution methodology to reinforce the weak subscription confidentiality, and 3) careful examination of various attacks on subscription confidentiality. General approach gives fine-grained key management and the cost for encryption, decryption, and routing is in the arrangement of subscribed attributes. Also, the assessments demonstrate that giving security is moderate w.r.t. 1) output of the suggested cryptographic primitives, and 2) delays caused throughout the development of the publish/subscribe overlay and the event distribution.*

Key Words: Security /subscribe mechanisms, Publish system, Authentication, Confidentiality.

1. INTRODUCTION

The publish/subscribe model developed from last few years as an effective device for distributed applications in which information must be scattered from event producers to event consumers i.e. from publishers to subscribers. Clients get certain sorts of occasions by applying channels on event contents called subscription. For each new event published the Pub/sub framework checks all events close to every present subscriptions and convey it to all clients for their coordinated subscription. Conventionally they were utilizing dealer networks for event routing from publishers to subscribers. In later frameworks, liaison-less routing infrastructure is utilized by making event forwarding overlay. [1]

In content based public subscribe systems data concerning an event (i.e. content of message) figures out where the message is conveyed. Senders send messages without knowing address of destination, with just some message noticeable to network. Receivers proclaim a query which is coordinated against published message. At that point the message is transmitted to all receivers whose question is coordinated by the content of the message. This strategy is valuable for various distributed applications like stock trade, movement control, publish detecting. Pub/Sub frameworks need to give security to these applications such access control and confidentiality.

The access control in pub/sub framework means only authenticated publishers are permitted to distribute events and just approved subscribers are permitted to get those events. Content of events are kept as secret and subscribers get that events without illuminating their subscriptions for the framework. Both publication and subscription confidentiality is required to decrease risk of spillage of events in systems. For that reason publisher and subscriber need to share private key, by utilizing public key foundation, which is definitely not desirable that it would debilitate the decoupling property of the model. In PKI, public keys of all subscribers are maintained by publishers for encryption of events. Correspondingly, to check authenticity of received events the subscribers must know the public keys. Conventional strategies for encrypting all message disregards the approach of content based framework. Consequently new technique is expected to route events to subscribers without knowing their subscriptions and authenticating them.

Public subscribe frameworks are given by most researchers yet less consideration is given on security of public subscribe frameworks. Existing methodology relies on traditional liaison network. This either manages security under constrained perspicuity, for example, by utilizing just keyword coordinating for routing events [2], [3] or relies upon semi-trusted merchant network [4] [5] [6]. In keyword search technique, events are routed in view of keyword in the message contents. This approach provides key administration yet does not give access control in adaptable way. However, in security issues of public subscribe frameworks how the subscribers are clustered is not specified.

In this paper we exhibit new way to provide authentication and confidentiality in public subscribe frameworks. The credentials are kept up in view of subscriptions of subscribers. We require keys to encrypt the event; private keys dispensed to the subscribers are named with credentials. There are set of credentials for publisher. The public key can be any arbitrary string in public key encryption. In such a plan there are four stages. In first setup stage, worldwide system parameters and a master key are created. In second, i.e. extraction, private keys are removed from master keys. In third, encryption, by using public keys the events is encrypted. In fourth, decryption, by using relative private keys the messages is decrypted. [7]

We build up an identity based encryption in which, if there is match amongst credentials and key then only the relative subscribers can decrypt event. Likewise it permits subscribers to check authenticity of received events. [8] In addition we handle issues with respect to subscription confidentiality for semantic clustering of events. A secure overlay maintenance protocol is intended to save the weak subscription confidentiality.

2. LITERATURE SURVEY:

W.C. Barker discussed about the “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher" [9] in the year 2012: TDEA is framed obtainable to be utilized by Federal organizations within the context of an entire security program comprising of physical security methodology and good data administration practices. TDEA could also be utilized by Federal associations to protect sensitive unclassified information. To keep up the confidentiality there is a need to protect information throughout transmission or in storage.

A.Sahai,J. Bettencourt, B. Waters explained about “Cipher text-Policy Attribute-Based Encryption" [8] in the year 2007: they have proposed a framework called as Cipher content Policy Attribute-Based Encryption for the unpredictable access control system on encrypted information. This method is utilized to keep the encrypted information secret in a situation where the capacity server is not secured. In the current Attribute-Based Encryption frameworks attributes are used to describe the encrypted information and furthermore characterize the strategies into client’s keys. In this proposed framework client’s qualifications are described by the attributes and an approach is controlled by the party that is encrypting the information for who can decode the encrypted information.

M.A. Tariq, B.Koldehofe, A.Altaweel, and K.Rothermel explained about “Providing basic security mechanisms in broker-less publish/subscribe systems" [10] in the year 2010.

This paper shows a novel way to provide confidentiality and authentication in a liaison-less content-based publish/subscribe framework. By adjusting the pairing-based cryptography components, the authentication of publishers and subscribers as well as confidentiality of events is ensured, to the necessities of a distribute/subscribe framework. Furthermore, it is an algorithm we used for clustering subscribers according to their subscriptions safeguards a weak idea of subscription confidentiality. Our approach gives fine grained key administration and the cost for encryption, decryption and routing is in the request of subscribed attributes.

A. Content Based Publisher /Subscriber (CBPS): Content based data model is used for routing the events from publishers to the relevant subscribers. Consider publisher/subscriber in a setting where there exists no committed liaison infrastructure. Publishers and subscribers contribute as associates to the upkeep of a self-organizing overlay structure. To authenticate publishers, we use the idea of advertisements in which a publisher reports beforehand the arrangement of events which it expects to publish [4].

B. Identity-Based Cryptography: Adi Shamir, proposed another sort of open key calculation in 1984. While public key frameworks have the innate issue of appropriating public keys and binds those public keys to a particular receiver, Shamir proposed mathematically creating the recipient's public key from his or her identity, then having the key server compute the required private key. This framework is called an

Identity-Based Encryption (IBE) algorithm [11]. In the IBE scheme, the sender Alice can utilize the receiver's identifier data which is represented by any string, for example, email or IP address; to encode a message [12].This approach would expel the requirement for public key queries or certificates.

C. Identity Based Encryption: In this paper, publishers and subscribers associate with a key server. They supply credentials to the key server and in turn get keys which fit the proclaimed capacities in the credentials. Afterwards, those keys can be used for encrypting, decrypting, and signing appropriate messages in the content based publisher subscriber system, i.e., the credential becomes approved by the key server. The keys are appointed to publishers and subscribers, and the cipher texts are marked with credentials. Generally, the identity-based encryption guarantees that a specific key can decrypt a specific cipher text only if there is a match between the key and credentials of the cipher text. Publishers and subscribers keep up discrete private keys for each authorized credential.

- Identity-Based Encryption (IBE) significantly simplifies the way of securing sensitive communications. Following example shows how Alice would send a protected email to Bob using IBE:

- There are two users initial one is Alice and second one is Bob. Alice encrypts messages and sends those messages to Bob along with her identity. Bob requests server for private key. Server allocates private key to Bob. Bob uses his private key to decrypt the received message.

3. SCOPE:

The pub/sub overlay proposed is like DPS system with alterations to confirm subscription confidentiality. In this paper, we assess performance and scalability of the proposed pub/sub system only with respect to the security mechanisms and discard different aspects. Specifically, we assess the performance of our system the overlay construction time and the event dispersal delays. We measure the average delay experienced by every subscriber of interface with an appropriate position in an attribute tree. Delay is computed from the time a subscriber forwards connection request message to a arbitrary peer in the tree till the time the connection is actually established. The assessments are performed just for a solitary attribute tree. It demonstrates that the average connection time (delay) increments with the amount of peers in the system because of the expansion in the height of the attribute tree (each new hop builds the network delay as well as time to apply security techniques).

4. PROPOSED SYSTEM:

Proposed System exhibits another way to give authentication and confidentiality in a liaison less pub/sub system. Our approach permits subscribers to keep up credentials as per their subscriptions. Private keys allotted to the subscribers are marked with the credentials. A publisher connects each encrypted event with a set of credentials. We accommodated identity based encryption (IBE) approaches 1) to guarantee that a specific subscriber can decrypt an event just if there is a match between the credentials related with the event and the key; and 2) to permit subscribers to validate the authentication of accepted events. Besides, we address the issue of subscription confidentiality within the sight of semantic clustering of subscribers. A weaker notion of subscription confidentiality is characterized and a secure overlay maintenance protocol is intended to safeguard the weak subscription confidentiality.

A. PROBLEM DEFINITION:

It incorporates two entities in the system: publishers and subscribers. Both the entities are computationally bounded and don't trust each other. Also, every one of the participant peers (publishers or subscribers) taking an interest in the pub/sub overlay system are straightforward and do not diverge from the planned protocols. In like manner, only authorized publishers propagate valid events in the system. Although, malicious publishers may act like the authorized publishers and spam the overlay network with fake and replicate events. We do not intend to resolve the digital copyright issue; consequently, authorized subscribers do not uncover the content of effectively decrypted events to different subscribers.

B. SYSTEM WORKFLOW AND ARCHITECTURE:

The traditional cryptosystems utilizes same keys for encryption and decryption. Both keys are kept will be kept secret. The issues of this conventional cryptosystems were distribution of keys and key administration. A paradigm is moved towards public key cryptosystem. In which diverse keys are utilized for encryption and decryption. One key is public and other is private. These plans also have some operational issues. For administration of keys Public key foundation is maintained. But conventional PKI needs to keep up huge number of keys. IBE gives other option to decrease amount of keys to store.

We use private key generator as trusted third party and also called as key server. Toward the begin first PKG produces pair of keys, public keys and private keys. The public key is accessible to clients. We call these keys as master public and private keys.

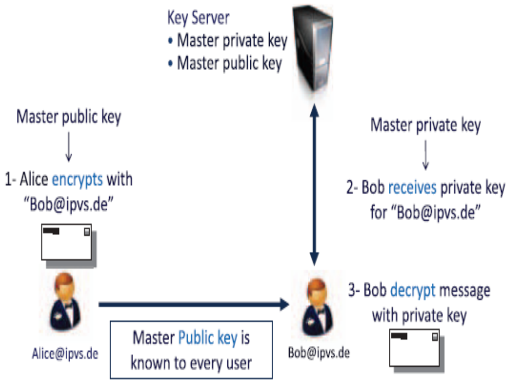

Key Server
• Master private key
• Master public key
Master public key
1- Alice encrypts with "Bob@ipvs.de"
Master private key
2- Bob receives private key for "Bob@ipvs.de"
3- Bob decrypt message with private key
Alice@ipvs.de
Master Public key is known to every user
Bob@ipvs.de

Figure 1: System Workflow

The figure 1 has been explained in following steps:

1) First sender, Alice makes plaintext message for receiver bob and we send this message from sender to receiver as shown in figure 1. To encrypt message, Alice uses few credentials that includes Bob's identity and cipher text is encrypted.

2) Bob receives cipher text from Alice, along with that some plain text information is also sent while transmission. The information which is transmitted is used for getting private key from PKG to decrypt message. Bob also required validating with PKG by sending credentials such as Identity of Bob. After that PKG transmits Bob's private key over a protected channel.

3) For example, E-mail address is used as public key.

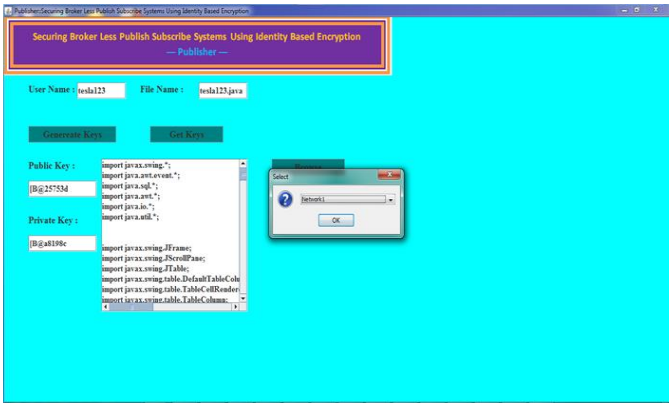
4) Bob uses his private key to decrypt cipher text to recover the plaintext message.

5) As PKG keeps up single Master public keys and Master Private Keys, so it can be utilized as smart card. A pairing based cryptography is utilized for execution of IBE. A mapping is built up between to cryptographic groups by means for bilinear maps.

5. CONCLUSION:

In this research paper, we have presented a modern technique to obtain authentication and confidentiality in a liaison-less content based publisher/subscriber system. The technique is most adaptable in respect of number of subscribers, publishers and the amount of kept up by them. Specifically, we have enlarged operations to relegate credentials to publishers and subscribers based on their subscriptions and advertisements. Private keys which are allocated to publishers, subscribers and cipher texts are labeled with credentials. We used methods from identity based encryption i.e. 1)To guarantee that a specific subscribers can decrypt an event only if they have same credentials linked with the event and its private keys.2)To permit subscribers to confirm the authenticity of received events. Besides, we built up a secure overlay maintenance protocol and suggested two event distribution techniques to protect the weak subscription confidentiality within the sight of semantic clustering of subscribers. The evaluations show the practicality of the proposed security systems and examine attacks on subscription confidentiality.

5. RESULTS AND OBSERVATIONS:


Publisher:Securing Broker Less Publish Subscribe Systems Using Identity Based Encryption

Securing Broker Less Publish Subscribe Systems Using Identity Based Encryption
— Publisher —

User Name : tesla123
File Name : tesla123.java

Public Key : [B@25753d
Private Key : [B@a8198c

```
import javax.swing.*;
import java.awt.event.*;
import java.sql.*;
import java.awt.*;
import java.io.*;
import java.util.*;


import javax.swing.JFrame;
import javax.swing.JScrollPane;
import javax.swing.JTable;
import javax.swing.table.DefaultTableColu
import javax.swing.table.TableCellRender
import javax.swing.table.TableColumn;
```

Select
Network1

Figure 2: Publisher Screen

In figure 2 we see a publisher screen where we generate and get keys by giving the system ip address and if there match i.e system ip address is same then it will generate keys after that we browse,upload the required file that is the file which publisher want to publish and he choose the deired network.

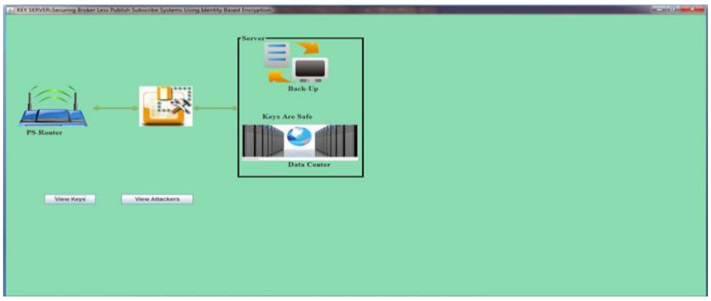
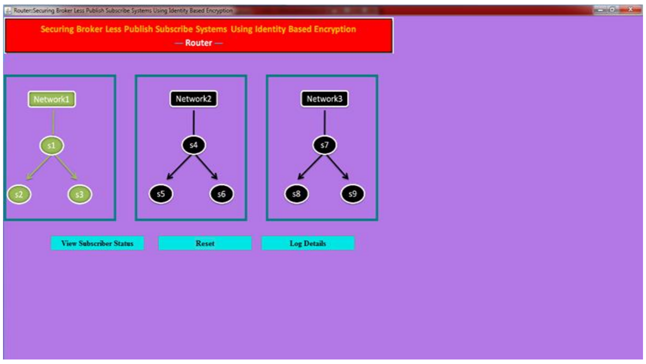

KEY SERVER-Securing Broker Less Publish Subscribe Systems Using Identity Based Encryption

Figure 3: key server

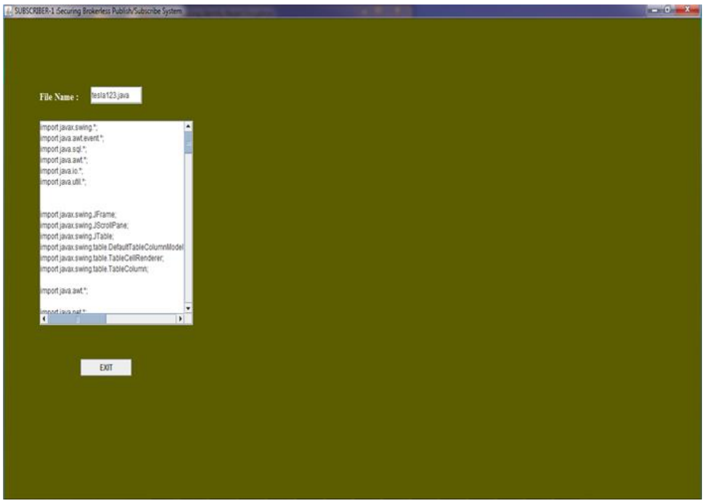
After selecting the desired network before publishing, the keys are sent to Data Center through router and key server for verification as shown in figure 3. If the keys are not attacked then the keys are in safe state else in not safe state.


Router:Securing Broker Less Publish Subscribe Systems Using Identity Based Encryption

Securing Broker Less Publish Subscribe Systems Using Identity Based Encryption
— Router —

Figure 4: Router screen

After verification process the uploaded file will be transmitted for the relevant subscribers as shown in figure 4.


SUBSCRIBER-1 :Securing Brokerless Publish/Subscribe System

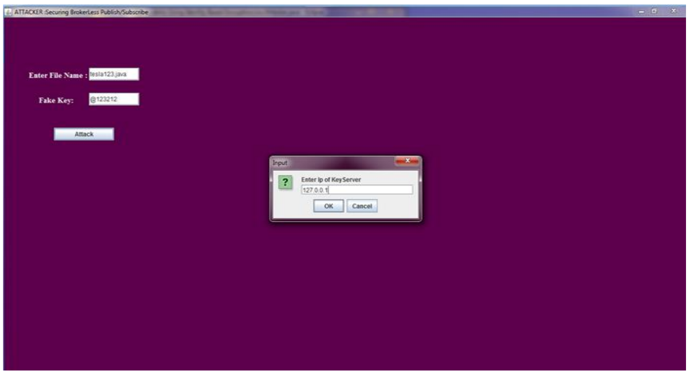
File Name : tesla123.java

```
import javax.swing.*;
import java.awt.event.*;
import java.sql.*;
import java.awt.*;
import java.io.*;
import java.util.*;


import javax.swing.JFrame;
import javax.swing.JScrollPane;
import javax.swing.JTable;
import javax.swing.table.DefaultTableColumnModel
import javax.swing.table.TableCellRenderer;
import javax.swing.table.TableColumn;

import java.awt.*;

import java.net.*;
```

Figure 5: Subscriber screen

In figure 5 we can see the subscriber where the publish data has been received to the subscriber without any modifications.

In figure 6 we see the attacker attacks the publisher using publisher private key.


ATTACKER :Securing BrokerLess Publish/Subscribe

Enter File Name : tesla123.java

Fake Key: @123212

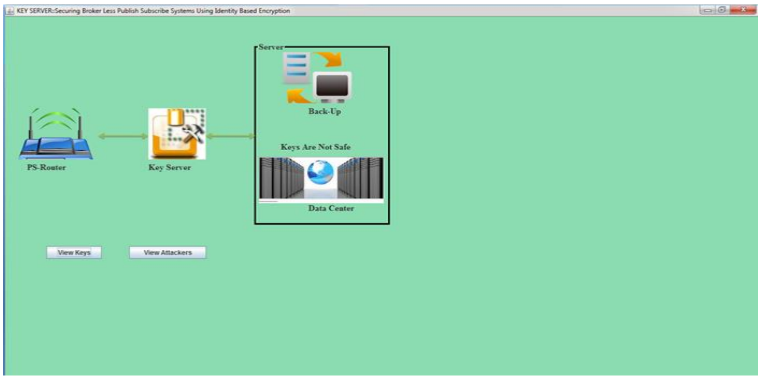
Input

Enter Ip of KeyServer

127.0.0.1

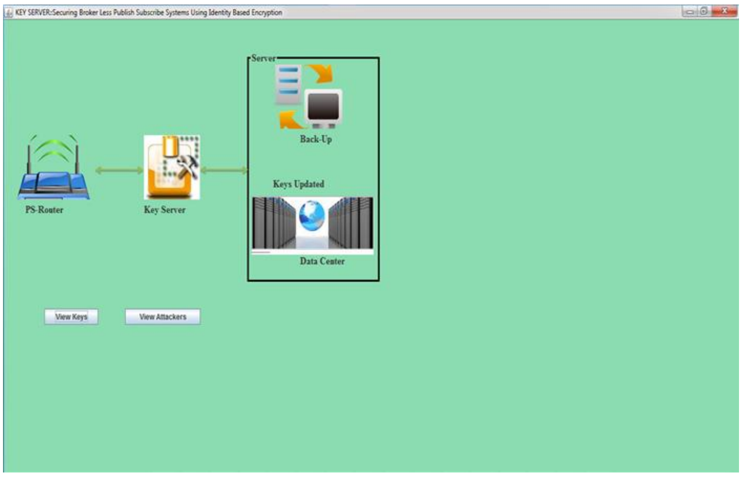
Figure 6: Attacker screen

After attacking there should be a message “keys are not safe” in the key server which is shown in figure 7.


KEY SERVER::Securing Broker Less Publish Subscribe Systems Using Identity Based Encryption

Keys Are Not Safe

Figure 7: Key server after attacking


KEY SERVER::Securing Broker Less Publish Subscribe Systems Using Identity Based Encryption

Keys Updated

Figure 8: keys updated by backup

We can see the keys are not safe in figure 7.In identity based encryption the keys which have been attacked will be updated using backup which we can see in figure 8.

REFERENCES

[1] E. Anceaume, M. Gradinariu, A.K. Datta, G. Simon, and A. Virgillito, "A Semantic Overlay for Self- Peer-to-Peer Publish/Subscribe," Proc. 26th IEEE Int'l Conf. Distributed Computing Systems (ICDCS), 2006.

[2] Antonio Carzaniga, Michele Papalini, Alexander L. Wolf "Content-Based Publish/Subscribe Networking and Information-Centric Networking".

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

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

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

[6] L. Opyrchal and A. Prakash, "Secure Distribution of Events in Content-Based Publish Subscribe Systems," Proc. 10th Conf. USENIX Security Symp., 2001.

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

[8] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, 2007.

[9] W.C. Barker and E.B. Barker, SP 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, technical report, Natl Inst. of Standards & Technology, 2012.

[10] M.A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel, Providing Basic Security Mechanisms in Broker-Less Publish/ Subscribe Systems, Proc. ACM Fourth Intl Conf. Distributed Event- Based Systems (DEBS),2010.

[11] A. Shamir, "Identity-Based cryptosystems and signature schemes", "CRYPTO", Springer, 1984.

[12] Joonsang Baek1 Jan Newmarch2, Reihaneh Safavi-Naini1, and WillySusilo1 "A Survey of Identity-Based Cryptography".