Securing Pub/Sub System Using Signcryption with Enhanced Energy Efficiency

U. Selvi[1], R. Karthika[2], B.Vidhya[3], K. Sriswathika[4]

Abstract—The basic security of content based pub/sub system provides authentication and confidentiality in publisher and subscriber. Due to loose coupling, its difficult to achieve the authentication of publisher and subscriber. As like, confidentiality of events and subscriptions conflicts with content-based routing. Here we are going to provide authentication and confidentiality in broker-less pub/sub systems, by using the paring based cryptographic mechanism, the authentication and confidentiality of publisher and subscriber of events is assured. This paper provides the signcryption which is a powerful primitive that offers both confidentiality and authenticity to important Messages. Signcryption performs simultaneously both digital signature and encryption.Honey Bee Behavior Inspired Particle Swarm Optimization Technique has been adapted for Resource Allocation and attain Energy Efficiency.

Index Terms— publisher, subscriber, content based, signcryption.

I. INTRODUCTION

We provide a new confidentiality authentication in content based pub/sub system. To prove this, paring based cryptographic [8] concept is been used to encrypt and decrypt the files. Signcryption, has a valid string which uniquely identifies the public key of the user. Alice encrypts the file, using master public key and sends the message to bob. Bob decrypt the same message by using master private key. Key Server maintains both public and private keys. Instead of identity based encryption [6],signcryptionconcepts are used. Signcryption performs the function of both digital signature and encryption.A secure signcryption scheme[7] should provide confidentiality, authentication, and should provide insider security too, i.e. even if the sender's private key is Compromised, an adversary should not be able to unsigncrypt the message and even with the receiver's private key, a forger should not be able to generate a fresh signcryption. Applications of signcryption are secure and authenticate email, e-commerce and m-commerce.

1. U.Selvi, Assistant Professor

Professional Group of Institutions

2. R.Karthika,B.E CSE

Professional Group of Institutions

3. B.Vidhya,B.E CSE

Professional Group of Institutions

4. K.Sriswathika, B.E CSE

Professional Group of Institutions

II. CONTENT BASED PUBLISH/ SUBSCRIBE

A. Review Stage

Content based pub /sub system is an interaction of the distribution system, allowing decoupled messaging through the CBPS infrastructure between two types of actors: (1)

subscribers, having interests in information is expressed as +subscriptions, and (2) publishers, producing information of interest as notifications. It is useful for large-scale distributed applications such as news distribution, market, to monitor the environment, traffic control, and public sensing. The event space, denoted by Ω, is composed of a global ordered set of d distinct attributes (T_i): $\Omega = \{T_1; T_2; \ldots T_d\}$. Each attribute T_i is characterized by a single name, its type of data, and it's Domain. The type of data can be any ordered type such as integer, floating point, and character strings. The domain describes the range $[L_i; U_i]$ of possible attribute values. A subscription filter f is a conjunction of predicates, i.e., $f = \{Pred_1 \wedge Pred_2 \wedge \text{------} \wedge Pred_j\}$. $Pred_i$ is defined as a tuple $(B_i;OA_i; X_i)$, where OA_i denotes an operator and X_i a value.

B. Attacker Model

Attacker model consist of two entities in the system 1) publisher 2) subscriber both entities are computationally bounded and do not trust each other. The authorized publishers are only able to disseminate the event. In cryptanalysis ,attacker model are a classification of specifying how much information a cryptanalysis has access to when attempting to break an encrypted message. In cryptography, a sending party uses a cipher to encrypt (transform) a top-secret plaintext into a cipher text, which is sent over an insecure communication channel to the receiving party. The receiving party uses his same top-secret knowledge of the cipher to decrypt the cipher text to obtain the plaintext. The top-secret knowledge required to decrypt the message is usually a short number or string called a key. In a cryptographic attack a goal between cryptanalyst analyses the cipher text to try to "halt" the cipher, to read the plaintext and obtain the key so that future enciphered messages can be read. It is usually supposed that the encryption and decryption algorithms themselves are

public knowledge and available to the cryptographer, as this is the case for recent ciphers which are published openly.

C. Signcryption

While a traditional PKI infrastructure requires maintaining for each publisher or subscriber a private/public key pair which has to be known between communicating entities to encrypt and decrypt messages, signcryption provides a promising alternative to reduce the amount of keys to be managed. In signcryption, any valid string which uniquely identifies a user can be the public key of the user. A key server maintains a particular pair of public and private major keys. The major public key can be used by the contributor to encrypt and send the messages to a user with any identity, for example, an e-mail address. To successfully decrypt the message, a receiver needs to obtain a private key for its identity from the key server. This shows the basic idea of signcryption. A contributor needs to know only a single major public key to communicate with any identity. Similarly, a receiver only obtains private keys for its own identities. Furthermore, an instance of central key server can be easily replicated within the network. Finally, a key server maintains only a single pair of major keys and, therefore, can be realized as an insolent card, provided to each participant of the system. Although identity-based encryption has been proposed some time ago, only recently pairing-based cryptography (PBC) has laid the foundation of practical implementation of signcryption. Pairing-based cryptography establishes a mapping between two cryptographic groups by means of bilinear maps. This allows the reduction of one tricky in one group to a different usually easier problem in another group. Here Bilinear maps are utilize to establishing the basic security mechanisms in the pub/sub system and, therefore, introduce here the main properties. Let GG1 and GG2 be cyclic group of order q, where q is some large prime. A bilinear map is a function ^e: GG1 _ GG1! GG2 that associates a pair of elements from GG1 to elements in GG2.A bilinear map satisfies the following conditions:

1. Bilinearity.
2. No degeneracy.
3. Computability.

D. Approach Overview

For providing security mechanisms in pub/sub, the principles of signcryption to support many-to-many interactions between subscribers and publishers. While the subsequently establish the implementation of our security methods in terms of a concrete variant called attribute-based encryption, it is main to comment that our method also benefits from other signcryption schemes. Publisher and subscriber are interacting with key server, and it also provides credentials to the key server, those keys are used to encrypt, decrypt and sign relevant message in content based pub/sub system. Credentials consist of two types 1) binary string 2) identity proof. The keys assigned to publishers and subscribers, and the cipher texts, are labeled with credentials. In particular, the signcryption ensures that a particular key can decrypt a particular cipher text only if there is a match between the credentials of the cipher text and the key. Publishers and subscribers maintain separate private keys for each authorized credential. Without contacting the key server or any other peer public key can be easily generated in the system. There is no need to interact the public key for encrypting the event and verification. Publisher does not know the relevant subscriber because it has loose coupling between the publisher and subscriber in the system. So the published event is encrypted with the public key of all promising credentials, which approves a subscriber to successfully decrypt the event. The encrypted events are than signed with the private key of the publisher. According to the relationship between the subscriptions, the overlay network is maintained. Each subscriber should know the subscription of its parent and child peers, according to the topology. When a new subscriber arrives, it sends the connection request (CR) along with its subscription to a random pier in the overlay network. Before it reaches the true pier to connect, the connection request is forwarded by possibly many peers in the overlay network.

E. Creation of Credentials

In creation of credentials there are three process i) Numeric Attributes ii) String Attributes iii) Complex Subscriptions.

1. Numeric Attributes

Here the event space composed a d-dimensional space attributes are processed, by spatial indexing approach it is hierarchically decomposed into regular subspace. The Subspaces are identified by a bit string of “0” and “1”s.And it is represented by dz_1 and covered by the dz_2,if dz_2 is a prefix of dz_1.The subscription can composed of several subspace. The credentials are assigned for every subspace and therefore it process two credentials. It represented by points and enclosed by subspace. The cipher text must be produced for every subspace to deliver the encrypted event and where it enclosed the peer of subscription which it positively decrypt the event. For large set of numeric attributes for the event space the credentials of subscriptions well are large. This affects the scalability of the system .We address this separately by decomposing the domain of attributes of subspace. This affects the scalability of the system.

2. String Attributes

By known domain of any ordered data type the spatial indexing technique is working in numerical attributes. It is usually have maximum number of characters. This allows them to have known limits. For more expressive string operations in credentials the tree are generated. Each node in the tree is labeled with a string. Each peer is assigned a particular

credential, which is same as its subscription. The leaf nodes correspond as tree. To deliver an encrypted event, a cipher text must be produced with the label of each node in the path from the leaf to the core of the tree, so that a peer whose subscription equals any of the labels should be able to successfully decrypt the event. In general, the number of nodes on the lengthier path from a leaf to the root of an irritated associated with a string attribute Bi is equal to Li, where Li is the length of the lengthier label assigned to a leaf node. Same mechanism can be used to produce credentials for suffix equals.

3. Complex Subscriptions

Complex subscription with founds on different points, a subscriber receives separate credentials and, thus, keys for each points. Using these keys, a subscriber should be able to positively decrypt any action with the corresponding points, if he is official to read the values associated with the points. In a content-based pub/sub system, a subscription defines a combination on founds. An action equals a subscription if and only if all of the founds in the subscription are fulfilled. To ensure action confidentiality, a subscriber must not be able to positively decrypt any event which equals only parts of its subscriptions.

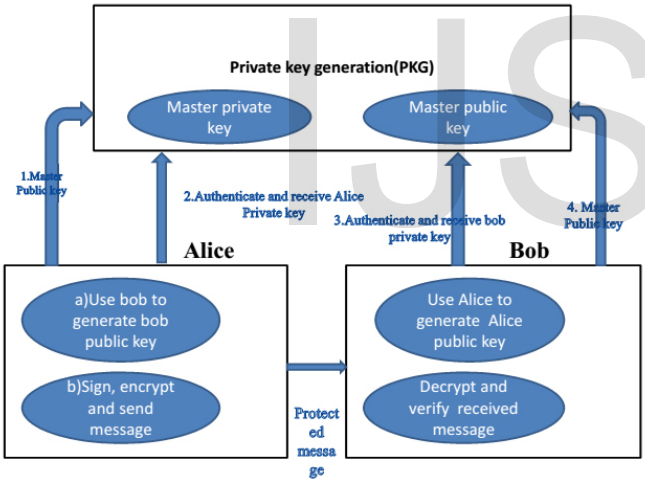

Fig.1: Process of signcryption

F. Subscription Cofidentiality

In broker-less pub/sub system, we achieve the subscription confidentiality.

1. Publish/Subscribe Overlay:

In pub/sub overlay, we taken the logical trees, here tree is associated with attributes subscriptions. According to the containment relationship between their credentials associated with the attribute, tree of the attributed are connected. Here the subscriber are handle more than one credentials by running multiple virtual peers on a single physical node. When a new subscribe are arriving the connection sends request along with credentials to random to random peer in the tree. The peer credentials compares the request to its own, if the peer credentials request the credentials and peer accommodate more children than it accepts children. Otherwise, it takes all children and parent peer, which it was received.

2. Weak Subscription Confidentiality:

Here we are going to provide strong subscription confidentiality in broker-less pub/sub system, because it maintains topology, it requires the subscription of parent as well as children.

3. Secure Overlay Maintenance:

The secure overlay maintenance , the subscriber are always connected with credentials for example, a subscriber with credential 11 can only connect to the subscribers with credentials 1 or 11. It is based on the idea in the tree. Without impolite the weak subscription confidentiality, this secure protocol maintains the pub/sub overlay topology. Secure Event Dissemination: Here we describe two strategies to route events (from publishers to the relevant subscribers) in the pub/sub overlay network without disturb the weak subscription confidentiality.

4. One-hop flooding (OHF):

In one-hop flooding ,parent assumes children with same credentials and it successfully decrypt an event, then children forward as the seine event and it successfully decrypted to all children. Here the overlay maintenance is done in worst case time. These strategies are available in online also. The result of one-hop flooding may receive false positive.

5. Multi credential routing**:**

In multi-credentials routing we reduce the false positive, by enabling parents to forward only those event on each attribute tree that match the credential of their children. Analysis of secure overlay maintenance and secures event dissemination algorithms to preserve weaker notion of subscription confidentiality as well as traffic analysis and timing attacks on subscription confidentiality.

G. Secure Event Dissemination

Secure overlay maintenance is maintained by the protocol adopted in [6] and signcryption is adopted for encryption prupose.

1. CertificatelessSigncryption without Pairing:

CLSC.Setup(1^R): The KGC takes the security parameter 1^R as input and performs the following for setting up the system:

• Chooses two big prime numbers p and q such that b|(a − 1).

• Selects an element r □ G Z*awith order b.

• Chooses a master private key□ G Z *b and computes the master public key $r_{pub}=r^C$.

• Chooses five cryptographic hash functions H1 : $\{0, 1\}^* \times Z^*_a \rightarrow Z^*_b$, H2 : $\{0, 1\}^* \times Z^*_a \times Z^*_a \rightarrow Z^*_b$,H3 : $\{0, 1\}^* \rightarrow Z^*_b$,H4 : $\{0, 1\}^* \rightarrow |M| \times Z^*_b \times Z^*_b$,H5 : $\{0, 1\}^* \rightarrow Z^*_b$, here M is the message space. The public parameters of the system, params={a,b,r,r_{pub}, H1,H2,H3,H4,H5}.

CLSC.PartialPrivateKeyExtract:

Given an identity, say ID_P of a user U_P, the KGC performs the following to generate the partial private key corresponding to IDP

• Chooses x_{A0}, $x_{A1} \epsilon R Z^*_b$

• Computes $X_{A0} = g^x_{A0}$ and $X_{A1} = g^x_{A1}$.

• Computes $q_{A0} = H1(ID_P, X_{A0})$ and $q_{A1} = H2(ID_P, X_{A0}, X_{A1})$.

• Computes $d_{A0} = x_{A0} + sq_{A0}$ and $d_{A1} = x_{A1} + {}^{sqA1.}$

Returns $d_A = <d_{A0}, d_{A1}>$ and $X_A = <X_{A0}, X_{A1}>$, the partial private keys securely to user U_A.

Note: It should be noted that the partial private key of a user is a Schnorr signature on the user'sidentity, signed by the KGC using the master private key.

CLSC.SetSecretValue: The user U_A chooses an element $y_A = G Z^*_b$ and keeps it as his secret value.

CLSC.SetPrivateKey: The user U_A sets his full private key $s_A = <y_A, d_{A0}>$

CLSC.SetPublicKey: The user U_A computes $Y_A = ry_A$ and sets his public key as $PK_A = <d_{A1}, X_{A0}, X_{A1}, Y_A>$The resulting public key is distributed widely and freely.

CLSC.Signcrypt: The sender $U_A$signcrypts a message m to a receiver U_B by performing the following:

• Chooses r_1, $r_2 = R Z^*_b$, computes $c_1 = g^{r1}$ and $c_2 = g^{r2}$.

• Computes $k1 = (Yq)^{r1}$ and $k2 = (X_{B0}.(r_{pub})^{qB0})^{r1}$.

• Computes d = H3(m, c_2, ID_A, ID_B, PK_A) and e = H5(m, c_2, ID_A, ID_B, PK_A) .

• Computes $v = (d.d_{A0} + e.y_A) + r2$.

• Computes $c3 = H4(k_1, k_2, ID_A, ID_B)$® (m||r1||v).

Now c = <c1, c2, c3> is the signcryption on message m to user U_B.

CLSC.Unsigncrypt: To unsigncrypt a signcryption $c = <c_1, c_2, c_3>$ from sender U_A, the receiver U_B does the following:

• Computes $k'_1 = (c_1)^{yB}$ and $k'_2 = (c_1)^{d}{}_{B0}$.

• Computes (m'||r'1||v')= c3 € H4(k'_1 , k'_2 , ID_A, ID_B).

• Checks whether $gr'_1 = c_1$.

• If so computes d' = H3(m', c_2, ID_A, ID_B, PK_A) and e' = H5(m', c_2, ID_A, ID_B, PK_A).

• Checks whether gv' =$((r_{pub})^{qA0'}.X_{A0})d'.(Y_A)e'.c2$.

If both the checks hold, m0 is output as the unsigncrypted message else outputs"Invalid".

Correctness: The correctness of the verification test $gr'_1 ?= c_1$ is straight forward. The second check alsopasses the verification if the signcryption is formed in a legitimate way which is shown below.

$Gv' = g(d_{A0}{}^{d'} + yA^{e'}) + r_2$

$= g(x_{A0}d' + sq_{A0}d' + yA^{e'}) + r_2$

$= g^{x}{}_{A0}d'.g^{sq}{}_{A0}d'.g^{yAe'}.g^{r2}$

$= ((r_{pub})^{qA0}.X_{A0})d'.(Y_A)e'.c_2$

Security of CLSC Scheme:

In this section, we provide the formal proof for the unforgeability and confidentiality of the CLSC scheme.

a. Type-I Unforgeability

Theorem 1. If an EUF-CLSC-CMA-I forger F_I has advantage ϵ_0 against CLSC scheme, asking qH_1 (i =1, 2, 3, 4, 5) hash queries to random oracles H_i (i = 1, 2, 3, 4, 5), q_{sc}signcryption queries, q_{us}unsigncryption queries, q_{pkr} extract secret value queries, q_{ppk} partial private key extract queries, q_{pk} public key request queries andq_{rpk} public key replacement queries, then there exist an algorithm C that solves the DL problem with advantage$\epsilon_0 > 1/9((1-\epsilon_0)^{qppk} .(1- q_{ppk}/q_{pk})/ q_{pk} - q_{us}/q_{sc}.(qH3+qH5+qsc)/2$, Where ϵ_0 is the advantage of an adversary breaking the Schnorr signature scheme.

b. Type-II Unforgeability

Theorem 2. If an EUF-CLSC-CMA-II forger FII has advantage ϵ_0 against CLSC scheme, asking qH_1(i = 1, 2, 3, 4, 5) hash queries to random oracles H_i (i = 1, 2, 3, 4, 5), q_{sc}signcryption queries, q_{us}unsigncryption queries, q_{pk}r extract secret value queries, q_{ppk} partial private key extract queries, q_{pk}publickey request queries and q_{rpk} public key replacement queries, then there exist an algorithm C that solves theDL problem with advantage

€≥ 1/g (è(1-qppk/qpk).(1-qrpk/qpk)/ qpk-qus/q-qsc.(qH3+qH5+qsc)/2^{n})

c. Type-I Confidentiality

Theorem 3.If an EUF-CLSC-CCA2-I adversary AI has advantage ϵ_0 against CLSC scheme, asking q_{Hi} (i = 1, 2, 3, 4, 5) hash queries to random oracles H_i (i = 1, 2, 3, 4, 5), q_{sc}signcryption queries, q_{us}unsigncryption queries, q_{pkr} extract secret value queries, q_{ppk} partial private key extract queries, q_{pk} public key request queries and q_{rpk} public key replacement queries, then there exist an algorithm C that solves the CDH problem with advantage

$€' \geq 1/q'^{4}.(1-\alpha)^{qppk}(1-qppk/qpk)-(qsc.(qH3+qH5+qsc)/2^{k})-qus/q)$

where, q'_4 is the number of tuples in the L_{H4} list having $<ID_A, ID\gamma>$and is the advantage of an adversary in breaking the Schnorr signature scheme.

d. Type-II Confidentiality

Theorem 4.If an EUF-CLSC-CCA2-II adversary AII has advantage $\epsilon_0$against CLSC scheme, asking q_{Hi} (i = 1, 2, 3, 4, 5) hash queries to random oracles Hi (i = 1, 2, 3, 4, 5), q_{sc}signcryption queries, q_{us}unsigncryption queries, q_{pkr} extract secret value queries, q_{ppk} partial private key extract queries, q_{pk}public key request queries and q_{rpk} public key replacement queries, then there exist an algorithm C that solves the CDH problem with advantage.
$\epsilon' \geq 1/q_4'(.(1-\alpha)^{qppk}(1\text{-}qppk/qpk)\text{-}(qsc.(qH3+qH5+qsc)/2^k)\text{-}qus/q$ where q_4' is the number of tuples in the L_{H4} list having <IDA, IDγ>.

H. Honey Bee inspired particle swarm optimization

As an extension of the work carried out by Prasanalakshmi et.al., [9], and with an aim to provide much secure resource allocation with improved energy efficiency, the Honey bee based particle swarm optimization technique has been adapted.

Table 1 represents the comparative analysis of the proposed Particle swarm optimization technique with that of Artificial Bee Colony algorithm based on the number of iterations and Table 2 represents the comparative analysis of the same algorithms based population size.

Iteration	Approach	Affinity	CPU time
50	PSO	3850.3	34
	ABC	3900.2	32
100	PSO	4521	54
	ABC	4700.82	51
150	PSO	3851.32	66
	ABC	3866	60
200	PSO	3658	87
	ABC	3985	87.5

TABLE 1 . Iteration based analysis

Pop. size	Approach	Affinity	CPU time
10	PSO	3850.3	34
	ABC	3900.2	32
20	PSO	4521	54
	ABC	4700.82	51
30	PSO	3851.32	66
	ABC	3866	60
40	PSO	3444	72
	ABC	3452	70
50	PSO	3658	87
	ABC	3985	87.5

TABLE 1 .Population sizebased analysis

III. Conclusion

A new approach to provide authentication and confidentiality in a broker-less content-based pub/sub system is discussed. The approach is highly scalable with the number of subscribers and publishers in the system and the number of keys maintained by them. A mechanisms is also been proposed to assign credentials to publishers and subscribers according to their subscriptions and advertisements. Private keys assigned to publishers and subscribers, and the ciphertexts are labeled with credentials. Also, certificatelesssigncryption scheme without pairing is introduced for the means of key generation every time of invoking in the random oracle model. The proposed scheme is more efficient since the scheme evades bilinear pairing. It has been proved that the security of the scheme with the strongest security notion for signcryption schemes, namely insider security. It as left as an open problem to construct certificatelesssigncryption scheme without pairing in the standard model for content based data sharing in Pub/Sub systems.

References

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

[2]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, pp. 2140-2153, 2011.

[3]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.

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

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

[6] Muhammad Adnan Tariq, Boris Koldehofe and Kurt Rothermel , "Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption" , IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.

[7] Y. Yu, B. Yang, Y. Sun, and S.-l. Zhu, "Identity Based Signcryption Scheme without Random Oracles," Computer Standards & Interfaces, vol. 31, pp. 56-62, 2009.

[8] B. Lynn, "The Pairing-Based Cryptography (PBC) Library," http://crypto.stanford.edu/pbc/, 2010.

[9]B.Prasanalakshmi,A.Kannammal, "Honey Bee Behavior Inspired Particle Swarm Optimization Technique for Adaptive Resource Allocation", International Journal of computer science and engineering communication(IJCSEC)December 2013.