ENHANCING SECURITY AND EFFICIENCY IN AGENT LESS PUBLISH/SUBSCRIBE SYSTEMS: A NOVEL APPROACH USING PAIRING-BASED CRYPTOGRAPHY AND LIGHTWEIGHT ENCRYPTION

[1]S.T.Saravanan, [2]T.Manigandan, [3]S.Indhumathi
[1]Assistant Professor, [2] Assistant Professor, [3]Assistant Professor
[1]Department of CSE, [2]Department of CSE, [3]Department of CSE
[1]Bharathiyar Institute of Engineering for Women, Salem, India,
[2]SRS College of Engineering and Technology, Salem, India
[3]Bharathiyar Institute of Engineering for Women, Salem, India,

Abstract: Because publishers and subscribers are not tightly coupled, achieving the fundamental security mechanism in a publish/subscribe system is extremely difficult. Through the adaptation of pairing-based cryptography, this paper presents a novel approach to provide confidentiality and authentications in a broker-less content-based publish/subscribe system. Additionally, it employs a lightweight encryption scheme, P-Coding, to provide confidentiality in an energy-efficient manner. Additionally, this article maintains the publish/subscribe system's weak subscription confidentiality. The overall method offers fine-grained key management, and the order of subscription attributes determines the cost of encryption, decryption, and routing. It lowers the energy that data encryption uses.

Keywords: identity-based encryption, broker-less, publish/subscribe, content-based, and security.

I. INTRODUCTION

The content of the information drives communication in the publish/subscribe system [8], not the identities of the producer (publisher) or consumer (subscriber). Publishers introduce events—information—into the system without the pertinent subscriber group's awareness. Additionally, subscribers use their subscription to express their interests without the publishers knowing. Traditionally, intermediary routing via a broker network has been used to guarantee this. Publishers and subscribers arrange themselves in a broker-less routing infrastructure in the most recent system. In this case, publishers and subscribers support the upkeep of the self-organizing overlay structure as peers.

Various methods for expressing interest in events have led to a wide variety of publish/subscribe system variations. The most powerful and expressive variation is content-based; in this case, subscriptions are described as the conjunction of elementary restrictions over the value of one or more attributes, and events are structured as a set of attribute/value pairs. Large-scale distributed applications like stock exchange, traffic control, news distribution, etc. can benefit greatly from this. Supporting methods for large-scale distributed applications' fundamental security requirements, including integrity, confidentiality, and authentication, should be offered by publish/subscribe[1]. In a pub/sub system, access control indicates that events can only be distributed throughout the network by verified publishers, and that authorized subscribers can only receive those events.

Most secure publish/subscribe methods now in use depend on the existence of a broker network. Thus, a novel method for ensuring confidentiality and authentication in a broker-less pub/sub system is presented in this study. With our method, publishers link a set of credentials to every encrypted event, and subscribers can keep their credentials up to date based on their subscriptions.

The credentials are identified on the private keys that are assigned to the publishers and subscribers. Identity-based encryption techniques are used in this context to: 1) guarantee that a certain subscriber can decrypt an event only insofar as the credentials linked to the event and the key match; and 2) enable subscribers to confirm the legitimacy of received events.Additionally, maintain the flimsy subscription confidentially. Additionally, we employ an energy-efficient method of event confidentiality provisioning called P-Coding, which is a lightweight encryption scheme. When considering encryption algorithms, P-Coding [2] uses less energy than others. Permutation encryption applied to coded messages is the fundamental concept of P-Coding.

II.LITERATURE SURVEY

Cipher text-Policy Attribute-Based Encryption is a system for the complicated access control technique on encrypted data that was introduced by J. Bethencourt, A. Sahai, and B. Waters [6]. This method ensures that encrypted data is maintained private even on unprotected storage servers. In this system, attributes are used to describe a user's credentials, and the party encrypting the data decides the policy for who can decrypt the encrypted data. In the previous research work, attribute-based encryption systems used attributes to describe the encrypted data and specify the policies into user's keys.

This work presents Cipher text-Policy Attribute Based Encryption, a system for implementing complicated access control on encrypted data. In multiple dispersed systems, access to data should be restricted to users who possess a specific set of qualifications or qualities. Thus far, the only way to enforce these standards is to use a trusted server to handle access control and store the data. Nonetheless, the confidentiality of the data will be jeopardized if any server hosting the data is compromised. The encrypted data can be kept private using ciphertext-policy attribute-based encryption approaches even if the storage server is untrusted, and the techniques are safe from collusion attacks. While in this system attributes are used to define a user's credentials and a party encrypting data chooses a policy for who can decrypt, previous attribute-based encryption systems utilized attributes to describe the encrypted data and built policies into user's keys.

M. Ion, G. Russello, and B. Crispo[3] have presented a pub/sub system that are loosely coupled where applications interact indirectly and asynchronously.Events are created by the publisher and distributed via a network of brokers to interested subscribers. By providing filters that the brokers employ to route events, the subscriber expresses its interest. Therefore, it should be avoided that publishers and subscribers have to divulge their secret keys to any system that safeguards the privacy of the events and the filters. Additionally, the broker should be able to do event filtering in order to route the events to the interested subscribers, and the mechanism should not limit the expressiveness of the filters. Since current methods don't adequately address these problems, they offer a mechanism in this article that will deal with every problem.

PSGuard was designed by M. Srivatsa and L. Liu[5] for safe event distribution in pub-sub networks. The key management methods make sure that the key management cost is independent of the total number of subscribers (N S) in the pub-sub system by disassociating keys from subscriber groups. To do this in two phases: (i) To begin, link an encryption key K(e) to an event e and an authorization key K(f) to a subscription filter f. To encrypt the secret attributes in an event e, use the encryption key K(e), and to decode the secret attributes in a matching event e, use the authorization key K(f). (ii) Map the encryption and authorization keys into a shared key space using hierarchical key derivation algorithms.

If and only if the event e satisfies the subscription filter f, the mapping makes sure that a subscriber can effectively derive an encryption key K(e) for an event e using an authorization key K(f) for the subscription filter f. J. Bacon. J. Singh and D. M. Eyers[4] provide a system architecture that has a specialized event-broker network that is shared by several management domains. They discovered that the architecture is suitable for a wide range of uses. Additionally, they presume that each domain has a secure server that controls credentials and activates roles in accordance with policy. Enforce RBAC on the publish/subscribe clients using the access control features included in the client-hosting brokers. Access control is generally easier to implement when event management functionality is divided into a specialized event service as opposed to a peer-to-peer method where the client and event service are collocated.The latter is unsuitable for critical data transmission applications. In order to maximize communication efficiency, they have assumed content-based routing as opposed to broadcast-based routing.

III. SYSTEM MODEL AND BACKGROUND

A .Based on content Release/Subscribe

There are two categories for publish/subscribe systems: type/topic and content/attribute based [4]. Topic-based publish/subscribe refers to the utilization of an event channel that is specific to a given topic or kind. The message content is taken into account in the content-based model. Based on the type and attribute value, a subscriber indicates the events they are interested in receiving. A global ordered set of d different attributes (Ai) makes up the event space represented by Ω, where ^{SM} ={A1,A2,….,Ad}. A combination of predicates, represented as f = {Pred1 ^ Pred2… ^ Predj}, is a subscription filter. Predi can be defined as a tuple (Ai, Opi, vi), where vi is a value and Opi is an operator. If and only if an event's attribute values match the associated subscription f, the event is matched against it.

B. Model of Attacker

The honest-but-curious model and the attacker model are comparable [7][1]. Publishers and subscribers in a pub/sub system lack mutual trust and are computationally constrained. They follow the established protocol and are also regarded as honest. That is, they do not drop events or convey them incorrectly; rather, they route the events in accordance with the protocol. Authorized publishers distribute legitimate events that occur within the system. However, dishonest publishers could pose as legitimate ones in order to flood the network with phony and repetitive events. Our intention is not to address the issue of digital copyright. Consequently, we presume that authorized subscribers don't tell other subscribers what is contained in events that have been successfully decrypted.Some subscribers are interested in learning about other subscribers' subscriptions and published events to which they are not permitted to subscribe. In a similar vein, reading events that are posted in the system piques the interest of certain publishers. Additionally, passive attackers have the ability to listen in on conversations and attempt to learn what events and subscriptions include. Lastly, we make the assumption that there are secure ways available for publishers and subscribers to get keys from the key server.

C. Security Objectives and Conditions

The two objectives of the suggested secure publish/subscribe system are scalability and security.[1][7]. Verification of Subscribers and Publishers: Events should only be published in the system by approved publishers in order to prevent publications that aren't qualified. In a similar vein, subscribers ought to only get messages that they are permitted to receive. i.e., the pub/sub system only permits participation from approved entities. Integrity and Confidentiality of Events: Only authorized subscribers should be able to view the events, and they should be shielded from unauthorized changes. Subscription confidentiality: Approved subscribers ought to get events that align with their interests without disclosing their subscriptions. A subscriber must get every event that corresponds with their subscription and is published by approved publishers in order to maintain subscription integrity. The safe publish/subscribe mechanism ought to grow in tandem with the quantity of users within the system. Maintaining scalability requires attention to these three factors: I The quantity of keys to be maintained and the subscription fee ought to be unaffected by the total number of users in the pub/sub system; ii) Rekeying overhead ought to be kept to a minimum.

D. Encryption Based on Identity

A party can encrypt data for a specific user using the public key encryption protocols that are currently in place, such as PKI [8]. Strong coupling exists between senders and recipients, meaning that before a sender may encrypt a message, the recipient needs to create a public/private key pair, have a certificate authority certify its public key, and then deliver it to the sender. PKI is ineffective for big subscriber counts since every event must be encrypted using a unique public key for each subscriber. Consequently, a method is required to allow any two users to interact safely and validate one other's signatures without exchanging private or public keys. Furthermore, maintaining subscription confidentially in a publish/subscribe system without a broker is quite difficult.

A viable substitute to lessen the number of keys that need to be managed is identity-based encryption [1][7]. Any legitimate string that may be used to uniquely identify a user can be that user's public key in identity-based encryption (IBE). One set of master keys, public and private, is kept on file by a key server. Publishers and subscribers utilize the master keys to encrypt and decrypt data. The sender can encrypt messages and send them to a user with any identity, such as an email address, by using the master public key.

The recipient must retrieve a private key for its identification from the key server in order to decrypt the message. The fundamental concept of identity-based encryption is depicted in Figure 1.

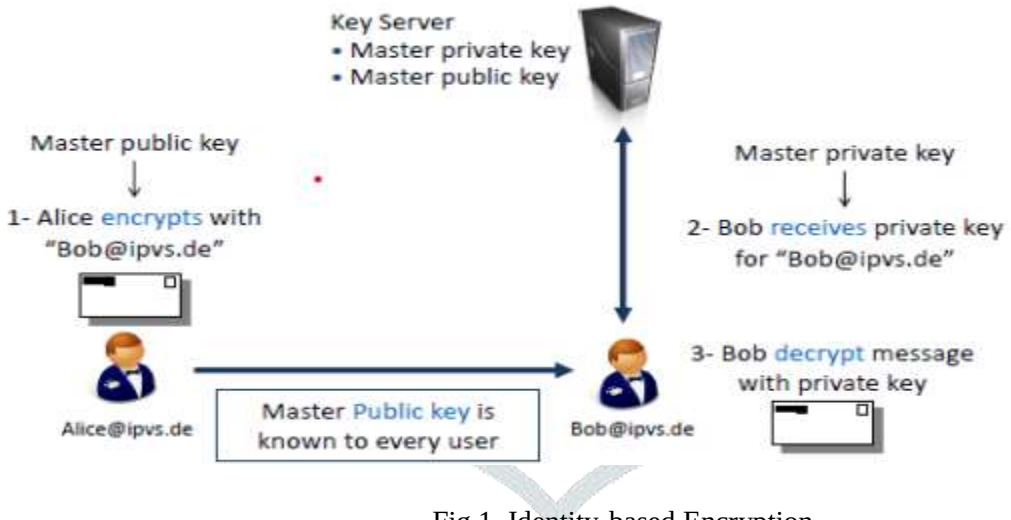

Fig.1. Identity-based Encryption

Identity-based encryption may now be implemented practically thanks to pairing-based cryptography [8]. It creates a mapping between two cryptographic groups in pairing-based cryptography. This makes it possible to reduce a problem from one group to a separate, typically simpler problem from another group. Bilinear maps are used to map between cryptographic groups; this method is used to establish the fundamental security features of a pub/sub network.

Principal characteristics of bilinear maps[6][1]: Assume that the cyclic groups G1 and G2 have order q, where q is a big prime. A function $\hat{e}$: G1 ×G1 →G2 that links two items from G1 to elements in G2 is known as a bilinear map. A bilinear map fulfills the subsequent requirements:

1. The bilinearity. For every u, v ∈ G1 and every x, y ∈ Z, $\hat{e}$ (ux, vy) = $\hat{e}$ (uy, vx) = $\hat{e}$ (u, v)xy.
2. The absence of degeneracy. For every u, v in G1, $\hat{e}$ (u, v) ≠ 1.
3. The ability to compute. $\hat{e}$ is computed efficiently.

E. Scheme for Lightweight Encryption P-Coding is a low-key encryption technique [2]. Permutation encryption is described as an instance of the traditional transposition cipher. P-Coding works by applying permutation encryption to communications that have been encoded. It could be necessary for the source to send a significant amount of data, length D, in dispersed content delivery. In this instance, the message or data is first divided into fixed-length blocks by the source. An index value is appended to each block. And PEF

(Permutation Encryption Function) is used to encrypt each and every block. Combine all of the encrypted blocks to create a single string, then encrypt it using PEF.

In P-Coding, we must first decrypt generations of packets before accessing the fitness of a permutation p. [2] O(nh2l) multiplications are needed for the decoding process, where n is the number of generations, h is the size of a generation, and l is the message length. The use of permutation encryptions confuses enemies who are listening in quite a bit. As a result, accessing the fitness of p in P-coding takes a lot longer. P-Coding requires very little computing power. P-Coding has been shown in recent research to contribute to reduced energy consumption in MANETs. When it comes to encryption systems, P-Coding uses less energy than others. Furthermore, P-Coding's encryption time is around one-third that of AES's. Greater throughput results from shorter encryption times. Additionally, it implies fewer CPU cycles, and less energy consumptions.

IV. OVERVIEW

The principles of identity-based encryption are used in pub/sub to provide security mechanisms [1] [8]. Attribute-based encryption, a general type of identity-based encryption, is the foundation upon which security measures are implemented. Specifically, the Ciphertext-policy Attribute-based encryption (CPABE) is modified here. Through the adaptation of pairing-based cryptographic techniques in terms of bilinear maps and the use of a lightweight encryption scheme called P-Coding, both the confidentiality of events and the authentication of publishers and subscribers are guaranteed [2]. By giving the key server their credentials, publishers and subscribers communicate with the key server. And afterwards obtains keys that match the declared capabilities listed in the credentials. These keys are employed in the content-based publish/subscribe system to encrypt, decrypt, and sign pertinent communications. That is, the key server authorizes the credential. A credential is made up of two components: identification evidence and a binary string that indicates an entity's capacity to send and receive events. Publishers and subscribers focus primarily on articulating a credential's capabilities, or how they might construct a credential together [1].

Credentials are allocated to the cipher texts and the keys given to publishers and subscribers [7]. Specifically, identity-based encryption makes sure that a given key can only decrypt a given cipher text if the cipher text's credentials and the key match. Publishers and subscribers keep different private keys for every credential that is allowed. The credential, the epoch for key revocation, and the symbol € {SUB, PUB} that separates publishers from subscribers are concatenated to create the public keys. Therefore, any peer in the system can easily generate the public keys without contacting the key server or other peers.The public key of every credential that is feasible is used to encrypt the published event, allowing a subscriber to successfully decrypt it. The publisher's private key is subsequently used to sign the cipher texts of the encrypted event, as illustrated in Figure 2.

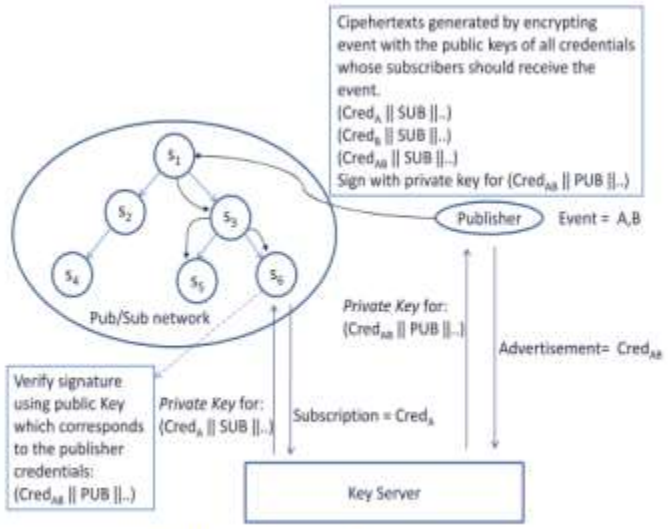

Fig. 2. Approach overview

The pub/sub overlay is thought to resemble a virtual forest made up of logical trees, with each tree having a characteristic assigned to it. The subscriber joins the trees that correspond to each attribute of its subscription once the publisher transmits its event to the trees linked to the attributes in the event. In accordance with the containment relationship between the credential and the attribute, the subscribers are linked to the tree. Near the base of the tree are the subscribers with coarser credentials, who send the events to subscribers with finer credentials. Every peer needs to be aware of its parent peers' and child peers' subscriptions in order to maintain the overlay topology. Therefore, strict subscription confidentiality is not possible. Thus, broker-free pub/sub systems solve the issue of inadequate subscription confidentiality. [8][1]

V. CONCLUSION

In this study, a method for supplying confidentiality and authentication in a pub/sub system without a broker for content was provided. When it comes to the quantity of publishers and subscribers in the system as well as the amount of keys that they will take care of. In this case, a system was created to allocate login credentials to publishers and subscribers based on their advertising and subscriptions. Publishers and subscribers are given private keys, and the cipher texts are marked with credentials. Additionally, P-Coding, a lightweight encryption method, and identity-based encryption techniques were adapted here. Identity-based encryption allows subscribers to confirm the legitimacy of received events and guarantees that a certain subscriber can only decrypt an event if the private keys and credentials associated with it match. Compared to other encryption schemes, a lightweight encryption system guarantees the least amount of energy consumption. Here, we anticipated that following the successful adoption of the suggested system, the broker less pub/sub system would demonstrate improved performance by preserving fundamental securities and for saving the energy.

REFERENCES

[1]. M. A. Tariq, B. Koldehofe, and K. Rothermel, "Securing Broker-Less Publish/Subscribe Systems Using Identity- Based Encryption," IEEE Transactions on parallel and distributed systems, vol. 25, no. 2, February 2014 .

[2]. P. Zhang, C. L.,Yixin Jiang, Y. Fan, and X. Shen, "A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks," IEEE Transactions on parallel and distributed systems, vol. 25, no. 9, September 2014.

[3]. 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 .

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

[5]. M. Srivatsa and L. Liu,"Secure Event Dissemination in Publish-Subscribe Networks," Proc. 27th Int'l Conf. Distributed Computing Systems, 2007 .

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

[7]. 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 Event-Based Systems (DEBS), 2010.

[8]. M. A. Tariq, B. Koldehofe, and K. Rothermel, "Non functional Requirements in Publish/Subscribe Systems,"