PROTECTING INVESTORS PRIVACY IN ONLINE TRADING SYSTEM

P.Bhargavi[1], E.Anuradha[2], V.Sabitha[3]

[1,2] UG Student, Dept. of IT, Jeppiaar SRR Engineering College, Chennai, Tamilnadu , India.
[3] Assistant Professor, Dept. of IT, Jeppiaar SRR Engineering College, Chennai

Abstract - *The web-based exchange platform is a built-up paradigm that uses a broker network to distribute information from financial specialists to shareholders in an approximately coupled manner. If broker gets compromised, and the intermediaries themselves are interested in finding out about the details, the delicate information could be leaked or disclosed to the outside party. A portion of the methodologies allow Brokers to do malicious activity. Furthermore, even when the interests are encrypted, if malicious brokers collude with malicious organizations, they will know the investors interests. In this project, we're presenting a trading system that ensures investor confidentiality in the presence of entrusted brokers by breaking broker operations. The investor's use of unique identity will provide a more safe trading environment. In addition, our approach avoids collusion attacks between entrusted brokers and malicious. The Pub encrypts the publication using the Key-Policy Attribute-Based Encryption (KP-ABE) scheme to protect the publications from unauthorized entities. Only the approved Subs can access the content of the publications in this way.*

1. INTRODUCTION

Publish and subscribe (pub / sub) systems allow data to be disseminated from publishers to interest subscribers in a loosely-coupled manner, where the data is distributed without directing contact between publishers and subscribers. Using a network of dedicated servers, referred to as brokers, publications, representing the data generated by publishers, are routed to interest subscribers. Such brokers form a network, and cloud service providers can easily offer them as Software as a Service (SaaS). A publication is usually composed of content and a collection of tags that identify keywords characterizing its content. Subscribers mark their preferences (a.k.a. subscriptions) through a series of restrictions on those tags in publications. Brokers match tags of the publications against registered interests to determine whether a subscriber is interested in receiving those publications. Then the broker selects and forward the publications to the expected subscribers. To order to protect sensitive information from entrusted brokers, some works recommend encrypting the publications, and subscriptions, so that, the brokers can still be fit the subscriptions against the tags of the publications without knowing their content. In this article, we provide a privacy-preserving pub / sub framework that effectively preserves subscriptions and avoids collusion attacks using a multi-broker setup without sacrificing the pub / sub model's loosely-coupled properties. Our proposal's innovation lies in the use of through broker forms to match and route publications towards the expected subscribers. The main idea is to split match operations (between encrypted subscriptions and publishing tags) into different phases, where a different type of broker executes -step. Every type of broker only processes partial information from which it cannot infer sensitive subscription information. Therefore, if a broker is compromised or a customer (or publisher) is in collusion, the subscriptions are still secured. Firstly, using a scheme such as Key Policy Attribute-Based Encryption (KP-ABE), the content of publications can only be accessed by the registered subscribers. Secondly, we introduce Searchable Encryption (SE) to ensure the keywords of publications aligned encrypted against the interests of subscribers. Third, the solution proposed is safe against collusion attacks between brokers and subscribers / publishers, thanks to the use of multiple brokers. Here, we emphasize that our previous work proposed the idea of using multiple types of brokers to protect against bribery attacks in pub / sub structures. This research expands our concept by offering a complex framework, a systematic securities review, and a thorough evaluation of results. In addition, we provide a motivational scenario, define security requirements for pub / sub systems, and provide a technical background on the cryptographic techniques applied, including the KP-ABE and SE systems.

2. RELATED WORKS

Raiciu et al.[1] implement a secure pub / sub system which ensures broker publications and subscriptions are kept confidential. By combining with different values-based SEs, their program supports encrypted filtering for equality interests as well as range interests.

Nabeel et al.[2] present both a symmetrical and asymmetric approach. Specifically, the publication payload is encrypted with a symmetric algorithm, and both tags and subscriptions are encrypted with the Paillier homomorphic cryptosystem, enabling brokers to suit privacy over encrypted data. This approach gives Articles and Subscriptions confidentiality.

Di Crescenzo et al.[3] create a 3-party pub / sub protocol that protects the privacy of subscriptions and publications while guaranteeing the system's efficiency. The protocol encrypts all interests and tags with 2-layer cryptographic pseudonyms, and semantically secures the encrypted tags and interests. A trusted third-party server is used to encrypt the second layer. Because of third party support, the broker is able to efficiently and safely check the equality between encrypted tags and interests. In fact, publishers and customers are not obligated to communicate directly.

Choi et al.[4]present a system for routing publications to expect subscribers that enable brokers to fit without knowing about the content of publications and subscriptions, and without directing communication between publishers and subscribers. This proposal relies on the Asymmetric Scalar-Product Preserving Encryption (ASPE) technique, which is a geometric transformation that supports number, minimum, maximum, and count functions other than equality filtering.

Borcea et al.[5] propose PICADOR, a stable topic based pub / sub system based on a proxy-re-encryption scheme. The authors apply a proxy-based lattice re-encryption scheme that allows partial homomorphic operations and preserves the pub / sub system's loosely-coupling property. That is, the brokers have tore-encrypt the publications, so that, the plain text of these publications can only be retrieved by the registered subscribers.

Tariq et al.[6] propose a stable broker-less pub / sub method, where honest-but curious publishers distribute the publications. Using the Ciphertext-Policy Attribute-Based Encryption (CPABE), ensuring that only registered subscribers can get the publications back. Additionally, they use Keyword Search (PEKS) Public-key Encryption to help to search operations to suit encrypted tags and interests. The publication is encrypted with each credential which matches the tags to ensure the decoupling rights.

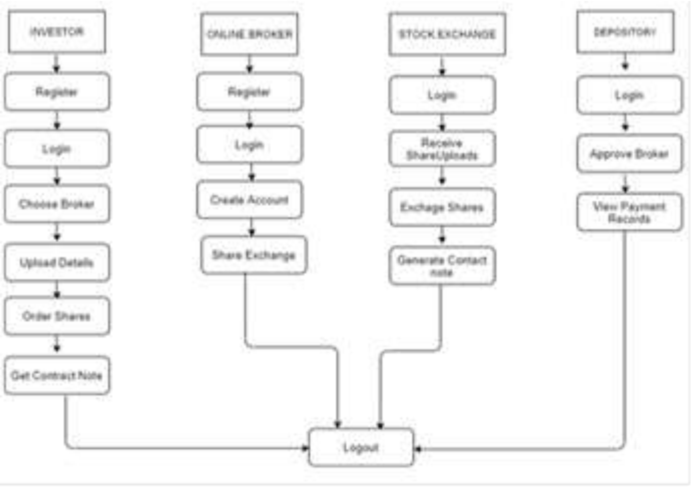
Yang et al.[7] implement a dual-policy ABE scheme that ensures a stable and efficient search of keywords in cloud-based pub / sub systems. The publisher establishes a policy of access over the keywords of the publications in this initiative, while the subscriber sets a different policy of access through its interests. The publishers are considered as completely trusted, the subscribers are malicious and the cloud server is concerned about that.

More recently, Pires et al.[8] have implemented a pub / sub routing engine that leverages the trustworthy environment of execution provided by shielded SGX enclaves. In this method, subscriptions are stored in the trusted SGX enclave, and the SGX enclave also performs the matching operation between interests and tags. In this situation, if the brokers are colluding with malicious publishers or subscribers, they cannot infer subscriptions from other subscribers because of the brokers are unable to access the details of the match operations because they are done in the enclave.

3. PROPOSED SYSTEM

Investor generates some interests in our proposed system and the associated tags. It encrypts both the tags and the appropriate data for the trading activity before it is released to the broker. Every investor determines according to their needs, so that only the partial data is obtained. The broker collection is employed with different functionalities and operated in various domains. The main idea of our solution is to divide the match operations between into three different phases where each phase is performed by a different type of broker. We allow at most two types of brokers to collude in our program, and are stilled able to protect the investor data information. Each type of broker knows only some partial information. Thus, even if malicious brokers collide with any two broker types (out of the three types supported in our solution), they cannot infer any investor's private data.

4. DATAFLOW DIAGRAM



5. SOLUTION

A. System Model:

Advertisers (Pub). The author creates the associated tags and publications. This encrypts both the tags, and the publication's payload before uploading to the broker.

Subscribers(Sub). Each subscriber defines a subscription according to their preferences, so that only those publications whose tags fulfill the subscription are received.

Shipper (B). The broker is responsible for screening and providing the interested Subs with the publications. Our approach consists of three types of brokers working together to process and distribute publications (p). Here we emphasize that different broker styles not only perform different functionalities but are also handled by different domains.

- Fidelity Authority (FA). The trusted authority is in charge of managing the Subs, and Pubs keys.

B. Threat Model:

We believe that the TA is fully trusted in this job, and that the channels between the TA and the Pubs / Subs are secure. We consider the following threat model in our system:

- Malevolent Sub. A malicious sub may attempt to access unauthorized publications by colluding with brokers, and may infer the interests of other Subs.

Malevolent Pub. A malicious Pub can attempt to infer the interests of Subs by injecting malicious publications and collaborating with brokers.

- Truthful but curious broker. The brokers are semi-trusted individuals. They follow the subscription review protocol but are curious about the quality of publications and interests. In addition, a broker may be colluding with any Sub or Pub to infer the preferences of other Subs. We need three types of brokers in our setting that is operated by at least three distinct non-colluding domains. In addition, we presume that the malicious Subs and Pubs may collude with two types of brokers controlled by two different domains, at most.

C. Our Approach:

In this article, we intend to provide a pub / sub service in the presence of hostile Subs and Pubs that could secure publications, and the interests of Subs from curious brokers. The Pub encodes the publication using the Key-Policy Attribute-Based Encryption (KP-ABE) scheme to protect the publications from unauthorized entities.

6. METHODOLOGY

A.KP-ABE

In KP-ABE, the cipher text is branded with a set of attributes whiles the private keys of the users are aligned with a policy of non-monotonic access. The consumer is able to decrypt the cipher text when the attributes encoded in the cipher text meet the access policy. In this function, the tags of each publication are taken by a Pub as the attributes set and encrypt the publications using KP-ABE. The private keys to decrypt the publications related to the interests of the Subs. Only those Subs whose interests satisfy the tags may retrieve the article. KP-ABE consists of four algorithms which follow:

- SetupKP−ABE(λ)− This algorithm is performed by the TA and takes the security parameter λ as an input. This creates both the public parameters PP and a master secret key MK.

- EncryptKP−ABE(PP, C, τ)− Message C, public parameters PP, and a collection of attributes as input are provided. It outputs the C-shaped cipher text. In this job, the tags for publishing are considered as the set attributes.

- KeyGenKP−ABE(MK, Ψ)− This algorithm takes the connection framework as its input, and the master secret key MK as its input. It produces a hidden sk-key. Sub's subscription in this work is regarded as the structure of the access. The TA also executes the algorithm.

- DecryptKP−ABE(sk, C)− The Sub's secret key for access structure Ψ and cipher text C will be used as inputs, and the message C will be output.

B. Searchable Encryption

In our solution we use the SUISE symmetric SE scheme to encrypt preferences and tags. On the one hand, SUISE promises authenticated subscriptions which are semi-secured. Thus, the broker cannot say whether Subs have the same interests or not simply based on their cipher text. In SUISE, on the other hand, matching between encrypted tags and interests is achieved with a keyed hash function which is much more effective than asymmetric encryption based schemes. In particular, its primitives AddToken and SearchToken are used to encrypt interests and tags, respectively, and the primitive Search is used to match encrypted tags with encrypted interests. Here, we emphasize that our solution is independent of any particular features provided by SUISE: other SE schemes which could effectively ensure confidentiality of interests and tags, could also be leveraged in our program. The basic SUISE that is part of our system include:

- GenSE(ÿ): This algorithm is also carried out by the TA. It takes a security parameter �as input, and generates a secret key k.

- AddTokenSE(k, I): The key k and the interest I are taken as input. It produces a searchable cryptographic value I by computing I=(HFk(I)(π),π), where π is a nonce, F:{ 0,1} l{ 0,1} l is a pseudo-random function (PRF), and H:{ 0,1} l{ 0,1} l is a random function (PRF).

- SearchTokenSE(k,τ): Given the secret key k and a tag, this algorithm produces a trapdoor τ∗ = Fk(τ) .

- Search SE(I∗,τ∗) It takes as input an encrypted interest I∗ = (μ,ν), and a trapdoor τ∗ of the tag. It outputs 1 if Hτ∗(ν) = μ, and 0 otherwise.

7. CONCLUSION

We propose a solution using three different broker types and breaking the corresponding process into three phases where each phase is performed by a different broker type. Even in the case of fraudulent subscribers (or publishers) colluding with up to two different types of brokers, the subscriptions of innocent subscribers cannot be inferred. Compromised brokers will deliberately tamper with the data in operation. For future work, we plan to examine approaches to detect broker malicious behavior, such as sending out publications to unintended subscribers or failing to forward the matched publications to expect subscribers. Overall our goal is to keep brokers accountable for their actions. The SE scheme (i.e. SUISE) used in our system supports only checking equality between encrypted tags and interests. We'll also consider supporting complex operations, such as range queries, for future work.

REFERENCES

[1] S. Cui, S. Belguith, P. D. Alwis, M. R. Asghar, and G. Russello, "Malicious organizations are in vain: protecting privacy in publishing and subscribing programs," in 2018, 17th International IEEE Conference on Trust, Security and Privacy in Computing and Communications/ 12th International Conference on Big Data Science and Engineering (TrustCom / BigDataSE), Aug 2018, pp. 1624–1627.

[2] D. E. Bakken, A. Bose, C. H. Hauser, D. E. Whitehead, and G. C. Zweigle, “Smart generation and transmission with coherent, real-time data,” Proceedings of the IEEE, vol. 99, no. 6, pp. 928–951, 2011.

[3] C. Esposito, M. Ciampi, and G. De Pietro, “An event-based notification approach for the delivery of patient medical information,” Information Systems, vol. 39, pp. 22–44, 2014.

[4] M. Cinque, C. Di Martino, and C. Esposito, “On data dissemination for large-scale complex critical infrastructures,” Computer Networks, vol. 56, no. 4, pp. 1215–1235, 2012.

[5] I. M. Delamer and J. L. M. Lastra, “Service-oriented architecture for distributed publish/subscribe middleware in electronics production,” IEEE Transactions on Industrial Informatics, vol. 2, no. 4, pp. 281–294, 2006.

[6] “Google cloud pub/sub,” https://cloud.google.com/pubsub, last accessed: November 27, 2018.

[7] “Yahoo data breach,” https://www.theguardian.com/technology/2016/ dec/14/yahoo-hack-security-of-one-billion-accounts-breached, 2016, last accessed: November 27, 2018.

[8] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. S. Shen, “Privacypreserving attribute-keyword based data publish-subscribe service on cloud platforms,” Information Sciences, vol. 387, pp. 116–131, 2017.

[9]M.R.Asghar,A.Gehani,B.Crispo,andG.Russello,“PIDGIN:Privacypreserving interest and content sharing in opportunistic networks,” in Proceedings of the 9th ACM symposium on information, computer and communications security. ACM, 2014, pp. 135–146.

[10] M. Ion, G. Russello, and B. Crispo, “Design and implementation of a confidentiality and access control solution for publish/subscribe systems,” Computer networks, vol. 56, no. 7, pp. 2014–2037, 2012.

[11] C. Esposito and M. Ciampi, “On security in publish/subscribe services: A survey,” IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 966–997, 2015.

[12] B. Shand, P. Pietzuch, I. Papagiannis, K. Moody, M. Migliavacca, D. Eyers, and J. Bacon, “Security policy and information sharing in distributed event-based systems,” Reasoning in Event-Based Distributed Systems, pp. 151–172, 2011.

[13] W. Rao, L. Chen, and S. Tarkoma, “Toward efficient filter privacy-aware content-based pub/sub systems,” IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 11, pp. 2644–2657, 2013.

[14] E. Onica, P. Felber, H. Mercier, and E. Rivi`ere, “Confidentialitypreserving publish/subscribe: A survey,” ACM Computing Surveys (CSUR), vol. 49, no. 2, p. 27, 2016.

[15] W. Rao, L. Chen, M. Yuan, S. Tarkoma, and H. Mei, “Subscription privacy protection in topic-based pub/sub,” in International Conference on Database Systems for Advanced Applications. Springer, 2013, pp. 361–376.