JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Secure and Efficient Product Information Retrieval in Cloud Computing

[1]A.Leela Prasanna, [2]Dr. K. V. Satyanarayana
[1]Pursuing M.Tech, [2]Associate Professor
[1]Department of CSE,
Raghu Engineering College, Visakhapatnam, India.

Abstract

The Publish and Subscribe (pub/sub) framework is a set up worldview to scatter the information from distributers to supporters in an inexactly coupled way utilizing an organization of devoted representatives. Be that as it may, touchy information could be presented to vindictive elements if specialists get bargained or hacked; or far more terrible, if intermediaries themselves are interested to find out about the information. A reasonable component to ensure touchy distributions and memberships is to encode the information before it is dispersed through the merchants. Cutting edge approaches permit dealers to perform encoded coordinating without uncovering distributions and memberships. Nonetheless, if malignant representatives plot with pernicious endorsers or distributers, they can get familiar with the interests of blameless supporters, in any event, when the interests are scrambled. In this article, we present a bar/sub framework that guarantees privacy of distributions and memberships within the sight of untrusted merchants. Moreover, our answer opposes conspiracy assaults between untrusted dealers and malignant supporters (or distributers). At long last, guarantee the security of distributions and memberships. To shield touchy data from untrusted agents[16], a few works propose to scramble the distributions and memberships so that the specialists can in any case coordinate [17]with the memberships against the distributions' labels without learning their substance. Accordingly, memberships and distributions are shielded from representatives. Nonetheless, it is as yet conceivable for malicious merchants to intrigue with endorsers and distributers[18]. In particular, a vindictive endorser could intrigue with an intermediary by unveiling the substance of her memberships. Thusly, regardless of whether the membership from a guiltless supporter is scrambled[19], the representative can in any case induce the substance by checking if the memberships from both an honest endorser and a malevolent endorser match a similar distribution labels[20]. Moreover, a pernicious distributer could mount an information infusion assault, i.e., distribute a phony distribution to gain proficiency with supporters' inclinations. In particular, a pernicious distributer can intrigue with a specialist to uncover the interests coordinating with the phony distribution. In this manner, to successfully guarantee the protection of memberships, it is likewise important to oppose plot assaults between agents, distributers, and supporters. The strategy against conniving supporters and merchants was first concentrated by Raoet al. Lamentably, there is little work done on arrangement assaults with regards to get bar/sub frameworks.

2. LITERATURE REVIEW

Publish subscribe in is an informing worldview that permits the making of adaptable and versatile appropriated frameworks. SIENA is an illustration of a well known substance based distribute[21] buy in framework, however numerous others have been created. The vast majority of the endeavours in this space concern unadulterated systems administration issues, similar to execution or versatility. Wang et al. break down the security issues and prerequisites that emerge in CBPS frameworks[22]. They predominantly distinguish old style security issues (like confirmation, respectability or secrecy) and adjust them to the CBPS case. However they don't give concrete or explicit answers for these new issues. Opyrchal and Prakash centre[24]around the classification issue just on the last leg from end-guide dealers toward supporters in a manner that is more proficient than bunch security regarding key administration[23]. However their plan accepts that agents are totally trust commendable. As of late two fascinating works concerning privacy in CBPS have been distributed. In the first place, creators centre around warning and membership privacy[24] as it were. They characterize the secrecy issues in a proper model and propose then couple of arrangements relying upon the membership and notice design. However the proposed coordinating with procedures are very exorbitant[25], since even the fundamental one highlighting balance tests

just is multiple times more slow than the convention without secrecy. In addition they expect that distributers and supporters share a mysterious [26]which decreases the decoupling of CBPS. Besides, in their aggressor model, just the merchants are straightforward[27] yet inquisitive, the distributers and endorsers are thought to be dependable. This supposition that is extremely solid on the grounds that the gathering of distributers and supporters might be exceptionally enormous. Such a plan doesn't secure supporters'protection[28] against other inquisitive endorsers for instance, let alone against malevolent supporters. Second, creators propose a particular key administration plan and afterward a probabilistic multi-way occasion[29] directing to forestall recurrence deriving assaults. In their danger model all hubs (distributers, endorsers and intermediaries) are thought truth be told yet inquisitive. The primary shortcoming of the plan is the prerequisite for a KDC which is a unified position that is confided in not to be interested and translate all the correspondence messages. Concerning content-based occasion steering, this plan thinks about that occasions have some routable ascribes which are tokenized to become pseudorandom chains and forestall word reference assault. They adjust the convention of Song et al. however, they don't persuade the utilization of this specific arrangement instead of simpler and lighter ones. Besides their method of guaranteeing security is through different way steering along these lines influencing the exhibition, while we ensure protection by cryptographic methods[30]. At long last, Opyrchal et al. manage security in CBPS, yet the focal point of the paper is principally on protection strategy the board and not on the plan of a crypto graphical convention to accomplish it.

Multiple encryption: Where creators propose onion steering, to restrict an organization's weakness to traffic investigation. It gives mysterious correspondence to HTTP through intermediaries utilizing the RSA commutative encryption plot. Autonomously, Pannetrat and Molva utilize various layer encryption for the dissemination of secret information from 1 source to a gathering of n hubs. This specific calculation guarantees multicast classification and it additionally forestalls the trade off of the entire gathering at whatever point a subset of hubs are undermined. Creators proposed a comparative methodology for information assortment in remote sensor networks where for this situation, n hubs are sending some information to 1 source, the sink. Notwithstanding classification, creators likewise exploit the innate homo morphic property in the hidden encryption method to guarantee total over scrambled information. Our plan joins both of these ways to deal with guarantee secure directing and henceforth supporter protection in then−to−n model similar to CBPS.

Private matching: The supporting of the protected gaze upward and secure table structure natives is a coordinating with activity utilizing scrambled information. Private coordinating has been presented for equity matches and reached out to more broad settings. However a cautious investigation of the issue shows that there is an unobtrusive yet significant contrast between private coordinating and the prerequisites of our plan. Private coordinating is without a doubt a two-party convention between a customer and a worker where the customer learns toward the end the data that he imparts to the worker, though for our situation the coordinating with activity must be performed by an outsider which has no influence over the information.

3. METHODOLOGY

3.1. Components

The segments of the P3S architecture are:

•Attribute-Based Access Control and Registration Authority (ARA): The ARA goes about as the certificate authority, and just interfaces with different segments during enlistment. During enrolment it furnishes the distributers and endorsers with data they need to distribute, including the metadata and predicate outline, CP-ABE and PBE keying material.

•Dissemination Server (DS): The DS sets up TLS passages to endorsers and distributers and monitors how to send data and affirmations to them. It gets PBE-scrambled metadata and CP-ABE-encoded payload from the distributers, and advances PBE-encoded metadata to enrolled supporters, and the CP-ABE-scrambled payload to the RS.

•Repository Server (RS): The RS stores CP-ABE encoded payloads alongside their related Globally-Unique-IDs (GUIDs), and sends the scrambled payload related with a GUID to an endorser upon demand.

•Predicate-Based Encryption Token Server (PBE-TS): The PBE-TS gets clear content membership interest (predicate) from the supporter, and returns the comparing PBE token to the endorser.

The P3S architecture is intended to oblige anonymization. On the off chance that accessible, sub-scribers contact PBE-TS and RS by means of the anonymization administration. P3S's essential security properties are free of anonymization, yet whenever consolidated, anonymization upgrades security assurance further by concealing the endorser personality to PBE-TS and RS.

3.2. High Level Overview

Fig. 1 illustrates the fundamental undeniable level P3S data stream. Distributers use CP-ABE to scramble payload with an arrangement that determines what ascribes are needed to unscramble it. Endorsers have ascribes that permit decoding of the CP-ABE encoded payload on the off chance that they fulfill the distributer's CP-ABE strategy. In this sense, CP-ABE gives a degree of access control to secure the classification of the payloads. Supporters acquire PBE tokens addressing their membership predicates. Distributers PBE scramble a ref-erence to the payload utilizing the related metadata and send the encoded metadata to endorsers, through the DS. Endorsers match their tokens against the scrambled metadata. An effective match yields the solitary data needed to recover the payload from the RS. Playing out the coordinating in the supporter joined with the utilization of PBE ensures the security of both endorser interest and substance metadata. The recovery demand is then sent through an anonymization administration.

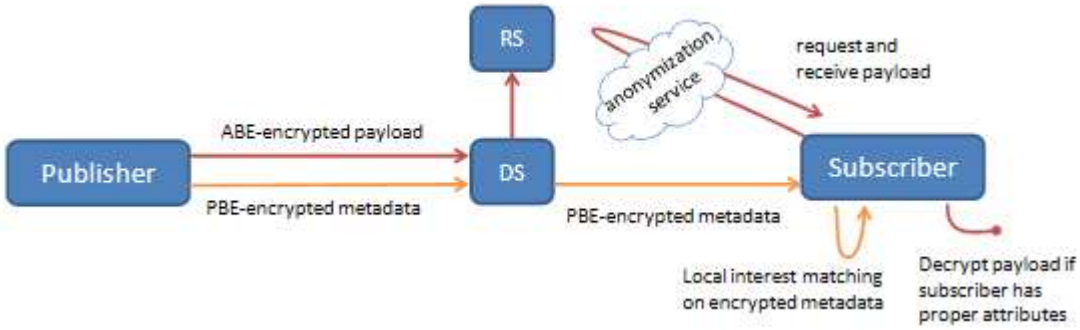

Fig. 1. P3S high level architecture

The CP-ABE encryption permits the distributer to control who can see the payload without requiring the distributer to know which supporter is accepting it. The PBE encryption permits the supporter of figure out which distributions match its inclinations without the framework revealing the metadata related with the distribution. Review that the entrance strategy in CP-ABE encryption is "free", and subsequently the entrance arrangements should just allude to credits that are protected to reveal to supporters that may neglect to decode the payload, for example, association names or endorser jobs. PBE encryption doesn't unveil the upsides of the ascribes used to scramble the information (but to the degree that a match with endorser predicates reveals it). In any case, our mongrel lease architecture doesn't give an instrument to limit the sorts of inquiries that an endorser can make.

3.3. Operation

Initialization: The ARA provides the subscriber with the PBE metadata format, i.e., field/value information for specifying subscription interests, contact information for the P3S services (RS, DS and PBE-TS) and their public key certificates, a CP-ABE secret key (SKC) based on the client attributes, which is used to decrypt payloads, and a certificate that indicates the participant is a subscriber.

Subscription: The subscriber generates a symmetric key and then uses the public key of the PBE-TS to encrypt the 3-tuple and sends it to the PBE-TS via the anonymization service. The PBE-TS decrypts the triple and, if the subscriber certificate is valid, computes the PBE token corresponding to the plaintext predicate. It then encrypts the token using the key and sends it back to the (unknown) subscriber via the anonymization service. This process allows the subscriber to obtain the token associated with its plaintext predicate while remaining anonymous to the PBE-TS providing the token.

Publication: The Publisher has a payload and associated metadata to be published. It generates a unique GUID from a large space (making it hard to guess) and then uses PBE encryption to encrypt that GUID. It sends this PBE-encrypted GUID to the DS which then forwards it to all the subscribers. The CP-ABE encryption specifies a policy that defines the attributes required by a subscriber if the payload is to be decrypted. The choice of this policy is outside of the scope of this paper, but could be determined by the payload metadata.

Deletion: Deletion is handled by the RS's garbage collection mechanism. The RS deletes the item corresponding to the identifier GUID after $T_{GUID} + T_G$. The reason for the configurable T_G parameter is to provide some accommodation for the uncontrollable delays in a distributed setting and slower consumers. For a strict interpretation of deleting based on publisher's intent T_G can be set to 0, which may result in considerably more failures to fetch the item for some (slower) clients with matched subscription.

Dimensional feature space, then to create optimized hyper-plane in feature space. Discriminant function is defined as follows:

$$F(x) = sgn[\sum_{i=1}^{n} \alpha i yi < \varphi(xi), \varphi(x) > + b] \quad \text{---------(EQUN 3.1)}$$

Usually we cannot know φ(x) specific expression, it is difficult to know the distribution and the number of high- dimensional space dimension after samples mapped to it. The hyper-plane can not to be solved in high-dimensional feature space. The dot product can be given directly by its corresponding kernel function, namely:

$$K(x_i, x_j) = <\varphi(x_i), \varphi(x_j)> \quad \text{-------(EQUN 3.2)}$$

Using the inner product $K(x_i, x_j)$ instead of the dot product in the optimal classification plane, we transform the original feature space to a new feature space to obtain a new optimization function as follows:

$$W(\alpha) = \sum_{i=1}^{1} \alpha i - \frac{1}{2} \sum_{i,j=1}^{1} \alpha i \alpha j yi K(xi, xj) \quad \text{----------(EQUN 3.3)}$$

Where $0 \leq \alpha_i \leq C$, $\sum_i \alpha i yi = 0$, $\alpha_i \geq 0, i=1,2,\ldots,l$

After solving the above problems, we can get the following optimal classification function:

$$F(x) = Sgn[\sum_{i=1}^{n} \alpha i y_i K(x_i, x) + b] \quad \text{----------(EQUN 3.4)}$$

4. RESULTS

In this segment, we assess the security and the exhibition of the plan. We first show that the proposed encryption instrument with different encryption layers guarantees classification against outside aggressors that don't take an interest to any systems administration or security activity and further show that it is arriving at its protection objective. In a work assessing the security of cryptosystems in the multi-client setting, Bellare et al. have basically shown that assuming a cryptosystem is secure in the feeling of in recognize capacity, the crypto framework in the multi-client setting, where related messages are scrambled utilizing various keys, is likewise secure. At the point when a message is scrambled with two free keys it is at any rate as secure as any individual encryption. Consequently, the plan is at any rate as secure as a one layer encryption. Besides, on account of the utilization of various encryption layers, the privacy of messages depends on the utilization of keys having a place with various clients. Messages are to be specific sent and constantly altered by the expansion and expulsion of encryption layers however they stay un open to specialists or busybodies consistently. Regardless of whether two supporters are buying in with a similar channel they can't tell so in light of the fact that every one scrambles it with various keys.

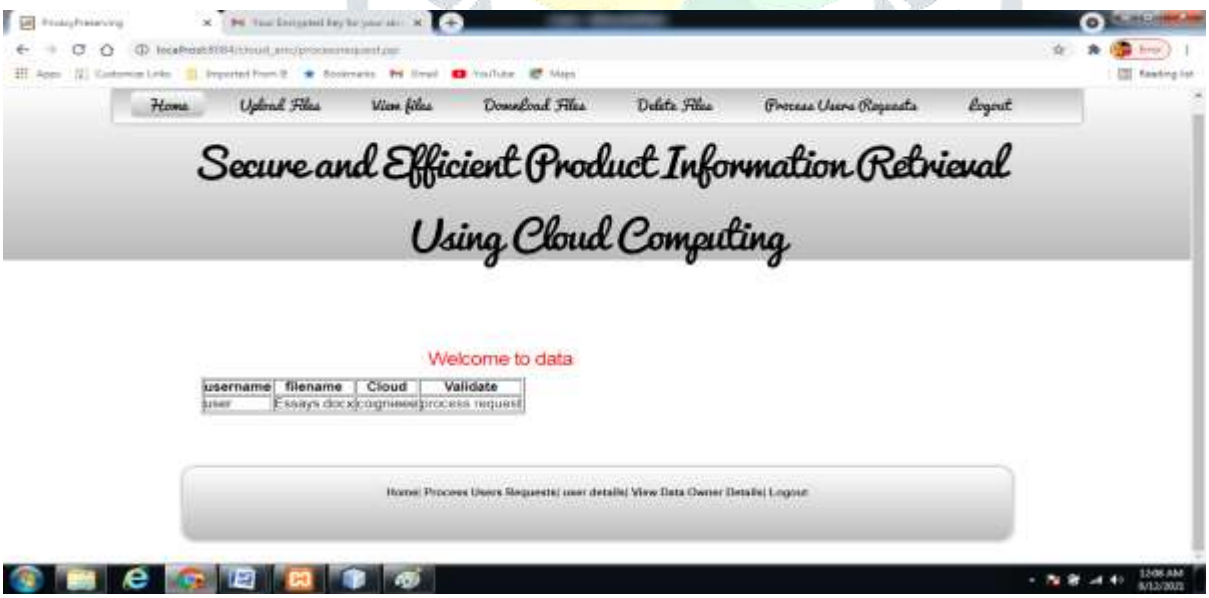

Figure 4.1 Permission Request Sending

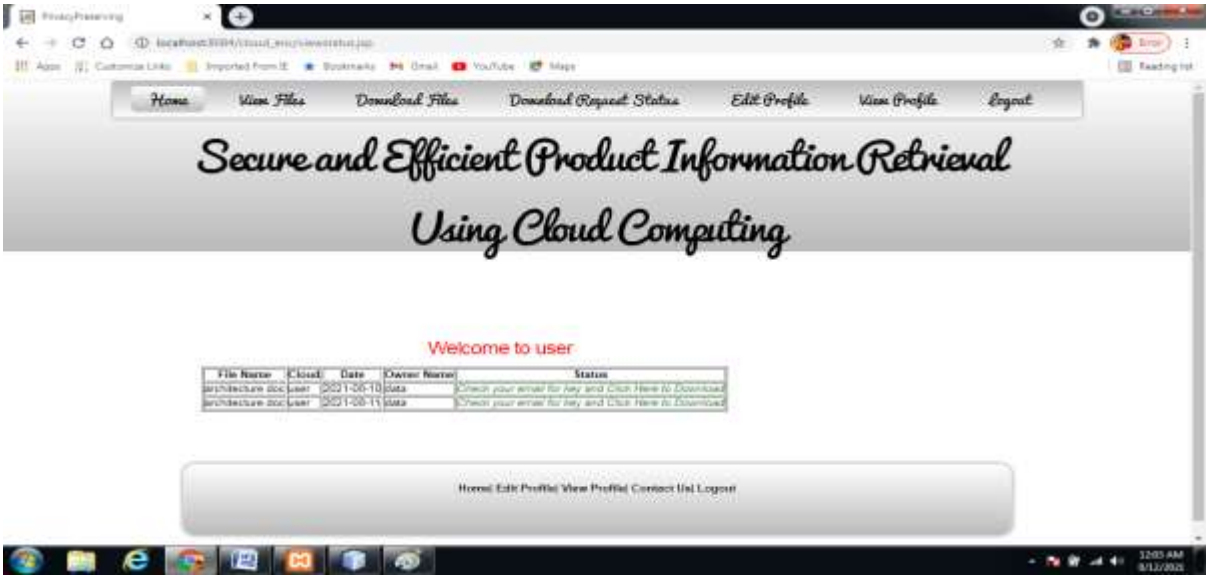

Figure 4.2 File Downoading to user

Our convention thus protects protection on account of secure and productive steering, also it gives the accompanying highlights:

1. The security of the Pohlig-Hellman cryptosystem depends on the discrete logarithm issue in a limited field of prime request which is hard when the example is obscure. Subsequently we can utilize similar key a few times and key administration is straightforward and neighbourhood.

2. The secure accumulation activity is extremely basic too since it is a basic equity test between two channels. On account of this safe collection of channels at each specialist, steering tables are streamlined.

3. Since there is no requirement for a common mystery, any hub can be an endorser. Agents for example can be sub-scribers and the protection of all supporters is as yet saved which is an extremely fascinating element particularly in a distributed climate.

Our convention depends on the utilization of two encryption layers to improve on the depiction. In the genuine yet inquisitive model this is ideal. Nonetheless if two continuous hubs, a hub and its parent, plot and henceforth share their own keying material, they can decode their kids hubs' memberships. Our plan considers a security against intrigue assault - which can happen just in a pernicious agent model-by expanding the quantity of encryption layers as portrayed . In this manner, the protection of the plan and its protection from arrangement assaults relies upon the decision of the quantity of encryption layers signified by r. The bigger qualities for r suggest a bigger number of hubs to connive to break it. In any case, with bigger, key stockpiling per hub turns into a weight and the key circulation overhead can affect the exhibition of the convention. Likewise conglomeration happens solely after r bounces so the bigger the r the less productive the collection system. The decision of r is henceforth a compromise that relies upon the situation and the geography of the organization.

5. COMPARATIVE ANALYSIS

Table 4.1 shows the diverse exhibition estimated by utilizing various boundaries. Condition is utilized to ascertain the precision, arrangement mistake and standard deviation of accessible dataset individually. Precision of strategic relapse is more noteworthy and arrangement

S. no	Algorithm	Cipher Length	Efficiency
1	ABE	64 bit	61%
2	CBABE	128bit	55%
3	RSA	32bit	64%
4	SHA1	16 bit	86%
5	Current Classifier	64bit	90%

Table 4.1 Comparative analysis of various algorithms and their accuracy

Table 4.1 shows the time cost of Enc calculation in KPSABES and KP-ABKS. To altogether assess the presentation of the file catchphrase encryption, we made three gatherings of various tests in our trial dataset. Figure 5a exhibits the time cost on one list catchphrase encryption while shifting the quantity of traits. We can see that the time cost of the two plans expanded directly with the quantity of characteristics, which is sensible since they are

both acquired from the first KP-ABE plot in . Table 4.1 shows the time cost of scrambling list catchphrases with various size when fixing the quantity of traits and information documents. The exploratory outcome shows that scrambling every one of the 320 file catchphrases separated from 2000 information records devoured around 290 s and 408 s in KPSABES and KP-ABKS, individually, when the quantity of properties was set to be 6. Table 4.1 shows that the quantity of information records had no impact on file watchword encryption in the two plans when fixing the size of file catchphrases and the quantity of qualities. As demonstrated in Table 4.1, t our KPSABES was more effective on list catchphrase encryption contrasted and KP-ABKS. Besides, the more prominent was the quantity of record catchphrases, the more clear was the benefit. This outcomes is sensible in light of the fact that encoding one list watchword in KP-ABKS required two more dramatic tasks than our plan as indicated by the calculation intricacy investigation. What's more, as demonstrated in the record catchphrase encryptions in the entire dataset were very tedious, yet was a one-time activity in light of the first KP-ABE plot, we plan a key-arrangement accessible characteristic based encryption conspire (KPSABES) to help effective watchword search and fine-grained admittance authority over encoded information. KPSABES is truly reasonable for the cryptography based information sharing stockpiling framework that needs the information access control and catchphrase based information looking. Not at all like the comparable KP-ABKS plot proposed in, based on the plan in, the plan doesn't need presenting any extra ciphertext parts and costly activities to help information looking. Thusly, KPSABES has some conspicuous benefits regarding capacity and calculation cost contrasted and KP-ABKS. What's more, broad investigations on a genuine dataset showed that KPSABES is better in numerous viewpoints than KP-ABKS, particularly in the inquiry execution. As our future work, we will consider the issue of proficient multi-watchword positioned search with fine-grained admittance power over scrambled information.

6. CONCLUSION

In this paper, we investigated security issues in content-based distribute/buy in networks. To tackle this issue with cryptographic instruments we investigated the connection among protection and privacy and recognized two important classification necessities, to be specific distributer and data secrecy. This drove us to the more broad issue of steering scrambled occasions utilizing encoded membership channels. This issue of secure directing requires two fundamental natives, to be specific structure of encoded steering tables with conglomeration of scrambled channels and secure gaze upward of scrambled occasions with scrambled steering tables to scatter the occasions proficiently. These two natives must be planned along with the other old style natives to address the protection saving directing which had no current arrangement. We at that point introduced an answer for this issue dependent on different layer commutative encryption. MLCE permits dealers to perform secure changes without approaching the information that is being moved. Agents can surely eliminate or add an encryption layer without obliterating the others and thus perform conglomeration, steering tables building or turn upward on private information secured by different layers. Protection is accordingly ensured among all hubs, including endorsers and listening in outcasts. Our answer utilizes the Pohlig-Hellman cryptosystem, and is the primary plan which empowers protection saving directing with no common mystery between end-clients. Consequently, key administration is simple and neighborhood. Another vital component of this convention is that it permits representatives to be supporters simultaneously while pre-serving protection of all hubs which is engaging for distributed applications. This convention can likewise be custom fitted to withstand arrangement assaults at a specific presentation cost. As future work, we mean to build up these plans by improving their adaptability in regards to the organization geography and the membership channel design. We might want to be sure to broaden membership channels envelop coherent articulations.

References

1.R. Agrawal, A. V. Evfimievski, and R. Srikant. Information sharing across private databases. In A. Y. Halevy, Z. G. Ives,and A. Doan, editors,SIGMOD Conference, pages 86–97. ACM, 2003.

2.G. Banavar, T. Chandra, B. Mukherjee, and Nagarajarao. An efficient multicast protocol for content-based publish-subscribe systems.Proceedings of 19th IEEE International Conference on Distributed Computing Systems, pages 262–272,1999.

3.M. Bellare, A. Boldyreva, and S. Micali. Public-key encryption in a multiuser setting: Security proofs and improvements.InEurocrypt 2000, pages 259–274. Springer Verlag, 2000.

4.K. P. Birman. The process group approach to reliable distributed computing.Commun. ACM, 36(12):37–53, 1993.

5.D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search. InEUROCRYPT,pages 506–522, 2004.

6.A. Carzaniga, D. S. Rosenblum, and A. L. Wolf. Design and evaluation of a wide-area event notification service. ACMTrans. Comput. Syst., 19(3):332–383, 2001.

7.L. Chmielewski and J.-H. Hoepman. Fuzzy private matching (extended abstract). In ARES, pages 327–334. IEEE Computer Society, 2008.

8.A. K. Datta, M. Gradinariu, M. Raynal, and G. Simon. Anonymous publish/subscribe in p2p networks. In IPDPS '03:Proceedings of the 17th International Symposium on Parallel and Distributed Processing, Washington, DC, USA, 2003.IEEE Computer Society.

9.M. J. Freedman, K. Nissim, and B. Pinkas. Efficient private matching and set intersection. In EUROCRYPT, pages 1–19,2004.

10.D. M. Goldschlag, M. G. Reed, and P. F. Syverson. Hiding routing information. Inin Information Hiding, pages 137–150.Springer-Verlag, 1996.

11.Y. Li, J. Tygar, and J. M. Hellerstein. Private matching. technical report IRB-TR-04-005, February 2004.

12.M. ̈Onen and R. Molva. Secure data aggregation with multiple encryption. In Wireless Sensor Networks, 4th European Conference, EWSN 2007, Lecture Notes in Computer Science, pages 117–132, Delft, The Netherlands, 29-31 January2007. Springer.

13.L. Opyrchal and A. Prakash. Secure distribution of events in content-based publish subscribe systems. InSSYM'01:Proceedings of the 10th conference on USENIX Security Symposium, pages 21–21, Berkeley, CA, USA, 2001. USENIX Association.

14.L. Opyrchal, A. Prakash, and A. Agrawal. Supporting privacy policies in a publish-subscribe substrate for pervasiveenvironments.JNW, pages 17–26, 2007.

15.A. Pannetrat and R. Molva. Multiple layer encryption for multicast groups. In The proceedings of CMS'02, Portoroz, Slovenia, September 2002.

16.S. Pohlig and M. Hellman. An improved algorithm for computing logarithms over gf(p) and its cryptographic significance. IEEE Transactions on Information Theory, 24(1):106–110, Jan 1978.

17.C. Raiciu and D. S. Rosenblum. Enabling confidentiality in content-based publish/subscribe infrastructures. Secure command Workshops, 2006, pages 1–11, 28 2006-Sept. 1 2006.

18.R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21:120–126, 1978.

19.D. X. Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypted data. Proceedings of the IEEE Symposium on Security and Privacy, pages 44–55, 2000.

20.M. Srivatsa and L. Liu. Secure event dissemination in publish-subscribe networks. In ICDCS '07: Proceedings of the27th International Conference on Distributed Computing Systems, page 22, Washington, DC, USA, 2007. IEEE Computer Society.

21.C. Wang, A. Carzaniga, D. Evans, and A. Wolf. Security issues and requirements for internet-scale publish-subscribe systems. In HICSS '02: Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 9, page 303, Washington, DC, USA, 2002. IEEE Computer Society.

22. Boneh, D.; Crescenzo, G.D.; Ostrovsky, R.; Persiano, G. Public-key encryption with keyword search. In *Advances in Cryptology—EUROCRYPT 2004*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 506–522. [**Google Scholar**]

23.Golle, P.; Staddon, J.; Waters, B. Secure conjunctive keyword search over encrypted data. In *Applied Cryptography and Network Security*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 31–45. [**Google Scholar**]

24.Ballard, L.; Kamara, S.; Monrose, F. Achieving efficient conjunctive keyword searches over encrypted data. In *Information and Communications Security*; Springer: Berlin/Heidelberg, Germany, 2005. [**Google Scholar**]

25.Boneh, D.; Waters, B. Conjunctive, subset, and range queries on encrypted data. In *Theory of Cryptography*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 535–554. [**Google Scholar**]

26.Yin, H.; Qin, Z.; Zhang, J.; Li, W.; Ou, L.; Hu, Y.; Li, K. Secure Conjunctive Multi-keyword Search for Multiple Data Owners in Cloud Computing. In Proceedings of the 2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS), Wuhan, China, 13–16 December 2016; pp. 761–768. [**Google Scholar**]

27.Sahai, A.; Waters, B. Fuzzy Identity-Based Encryption. In *Advances in Cryptology—EUROCRYPT 2005*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 457–473. [**Google Scholar**]

28.Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07), Berkeley, CA, USA, 20–23 May 2007; pp. 321–334. [**Google Scholar**]

29.Cheung, L.; Newport, C. Provably Secure Ciphertext Policy ABE. In Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 29 October–2 November 2007; pp. 456–465. [**Google Scholar**]

30.Waters, B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Public Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 53–7

31.Lewko, A.B.; Waters, B. Decentralizing attribute-based encryption. In *Advances in Cryptology—EUROCRYPT 2011*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 547–567. [**Google Scholar**]