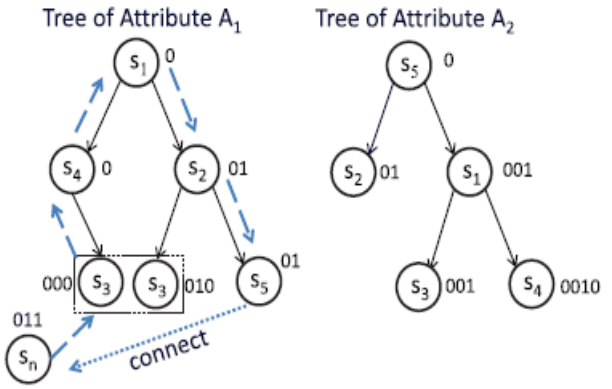

Figure 2: Publish/Subscribe system with two numericattributes

A different random key SW is used for the generation ofeach cipher-text to avoid any information leak to the peerwho has successfully decrypted one of the cipher-text and,thus, has recovered the random key SW. Otherwise, thepeer can try to generate cipher-text by encrypting the(recovered) SW with public keys for Olog2Zip credentials and can easily determine the random cipher-text in the connection request and, thus, the credentials of the requesting subscriber s. Finally, to avoid an attacker to generate arbitrary connection request messages and try to discover the credential of other peers in the system, the connection request is signed by the key server. This step needs to be performed only once, when a newly arriving subscriber authorizes itself to the key server in order to receive private keys for its credentials.

Algorithm 1. Secure overlay maintenance protocolat peer sq.
1: upon event Receive (CR of s new from sp) do
2: if decrypt request (CR)= = SUCCESS then
3: if degree (sq) == available then //can have child peers
4: connect to the s new
5: else
6: forward CR to {child peers and parent} - sp
7: if decrypt request (CR)= = FAIL then
8: if sp = =parent then
9: Try to swap by sending it own CR to the snew.
10: else
11: forward to parent

A child peer sq receives CR (of subscriber snew) from the parent sp only if the parent cannot accommodate more children. If sq cannot be the parent of snew, i.e., snew's credential is coarser than that of sq, then it tries to swap its position with snew by sending its own connection request (cf. Algorithm 1, lines 7-9). However, if none of the children of parent sp can connect or swap with snew, then there is no containment relationship between the credentials of the children and snew. In this case, a parent should disconnect one of its children to ensure the new subscriber is connected to the tree.

5. Conclusions

In this research paper, I have presented a new method to provide authentication and confidentiality in a broker-less identity based pub/sub system. The approach is highly scalable in terms of number of subscribers and publishers in the system and the number of keys maintained by them. In particular, we have developed mechanisms to assign credentials to publishers and subscribers according to their subscriptions and advertisements. Private keys assigned to publishers and subscribers, and the cipher-text are labeled with credentials. I adapted techniques from identity-based encryption 1) to ensure that a particular subscriber can decrypt an event only if there is a match between the credentials associated with the event and its private keysand 2) to allow subscribers to verify the authenticity of received events. Further more, we developed a secure overlay maintenance protocol and proposed two event dissemination strategies to preserve the weak subscription confidentiality in the presence of semantic clustering of subscribers. The evaluations demonstrate the viability of the proposed security mechanisms and analyze attacks on subscription confidentiality.

References

[1] M. Jelasity, A. Montresor, G.P. Jesi, and S. Voulgaris, "PeerSim: APeer-to-Peer Simulator," http://peersim.sourceforge.net/, 2013.
[2] W.C. Barker and E.B. Barker, "SP 800-67 Rev. 1. Recommendationfor the Triple Data EncryptionAlgorithm (TDEA) Block Cipher,"technical report, Nat'l Inst. of Standards & Technology, 2012.
[3] M. Nabeel, N. Shang, and E. Bertino, "Efficient Privacy PreservingContent Based Publish Subscribe Systems," Proc. 17th ACM Symp.Access Control Models and Technologies, 2012.
[4] M.A. Tariq, B. Koldehofe, G.G. Koch, I. Khan, and K. Rothermel,"Meeting Subscriber-Defined QoS Constraints in Publish/SubscribeSystems," Concurrency and Computation: Practice andExperience, vol. 23, pp. 2140-2153, 2011.
[5] M. Srivatsa, L. Liu, and A. Iyengar, "EventGuard: A SystemArchitecture for Securing Publish-Subscribe Networks," ACMTrans. Computer Systems, vol. 29, article 10, 2011.
[6] 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.
[7] S. Choi, G. Ghinita, and E. Bertino, "A Privacy-EnhancingContent-Based Publish/Subscribe System Using Scalar ProductPreserving Transformations," Proc. 21st Int'l Conf. Database andExpert Systems Applications: Part I, 2010.
[8] M. Ion, G. Russello, and B. Crispo, "Supporting Publication andSubscription Confidentiality in Pub/Sub Networks," Proc. SixthInt'l ICST Conf. Security and Privacy in Comm. Networks SecureComm),2010.
[9] H.-A. Jacobsen, A.K.Y. Cheung, G. Li, B. Maniymaran, V.Muthusamy, and R.S. Kazemzadeh, "The PADRES Publish/Subscribe System," Principles and Applications of DistributedEvent-Based Systems. IGI Global, 2010.
[10] A. Lewko, A. Sahai, and B. Waters, "Revocation Systems with VerySmall Private Keys," Proc. IEEE Symp. Security and Privacy, 2010.

[11] B. Lynn, "The Pairing-Based Cryptography (PBC) Library,"http://crypto.stanford.edu/pbc/, 2010.
[12] F.P. Miller, A.F. Vandome, and J. McBrewster, Advanced EncryptionStandard. Alpha Press, 2009.
[13] A. Shikfa, M. O ¨ nen, and R. Molva, "Privacy-Preserving Content-Based Publish/Subscribe Networks," Proc. Emerging Challenges forSecurity, Privacy and Trust, 2009.
[14] Y. Yu, B. Yang, Y. Sun, and S.-l. Zhu, "Identity Based SigncryptionScheme without Random Oracles," Computer Standards & Interfaces,vol. 31, pp. 56-62, 2009.
[15] J. Bacon, D.M. Eyers, J. Singh, and P.R. Pietzuch, "Access Controlin Publish/Subscribe Systems," Proc. Second ACM Int'l Conf.Distributed Event-Based Systems (DEBS), 2008.

Author Profile

Sayaram Shingote received the B.E. degree First Class with Distinction in Information Technology and M.E. in Software Engineering from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad. Area of interest is Information security.

Prof. Syed Akhter, Head of Department of Computer Engineering & M.E. Coordinator in Aditya Engineering College, Beed (Maharashtra).