A Novel Approach for Security Policy Integration and Conflict Reconciliation among Collaborating Organizations in a Ubiquitous Environment

Beneyaz Ara Begum¹, Animesh Tripathy²

¹Research Associate, Department of CSE, CET, BPUT, Bhubaneswar, INDIA.
²Associate Professor, Department of CSE, KIIT University, Bhubaneswar, INDIA.
¹beneyazarbegum@hotmail.com , ²animesh_tripathy@hotmail.com

EXTENDED ABSTRACT

Present data sharing and integration among various collaborating organizations requires a central and trusted authority to check the users’ requests before allowing the request to pass to the centralized repository to collect data from all data sources and then integrate the collected data. Due to the heterogeneity and dynamic nature of the ubiquitous computing environments it is critical to generate an integrated security policy set to govern the interactions among collaborating organizations during the collaboration. Security policy integration and conflict reconciliation (SPICR) layer is introduced between the user application and the repository for security policy negotiation and conflict reconciliation to collect and integrate data. With our proposed layer, data sharing services can update and control the access and limit the usage of their shared data, instead of submitting data. Our layer improves data sharing and efficiency of the centralized repository and makes the system scalable with little human intervention. The proposed layer performs security policy integration based on similarity policy adaptation algorithm and negotiation-based policy. In our system, the SPICR layer supports the repository to collect only the required data for users’ integration requests. We assume that the SPICR layer will correctly evaluate the users’ request to generate integration requirements and pass it to the repository to construct the query plans for users’ integration requirements, decompose query plans, discover and fetch data from distributed data sharing services, integrate all data together, and, finally, return the final results to users. The SPICR has four major components namely: Security policy vocabulary generator, Security policy adapter, Dynamic security policy Integrator and Negotiation-based conflict Reconciler. The user provides his/her public key and the integration requirements of data. Apply encryption algorithm for all values of selected attribute. Then the Security Policy vocabulary generator checks the policy specifications for the requested user. The generator resolves ambiguity among the security policies. The Security policy Adapter adapts the existing security policies for the extended user set. It decides whether to grant the user to access the data or deny the user. The Dynamic Security policy Integrator integrates security policies to generate a new set of security policies that is not present in either of collaborating organizations. The Negotiation-based conflict Reconciler resolves the conflict between the security policies and makes a compromise by selecting the weakest security policy in the policy hierarchy. Once the user is granted access to the data, the query plan wrapper of repository generates a query plan graph and then decomposes it to a set of sub trees using the Decomposition Algorithm and sends the sub trees to query plan executor. Data Sharing Algorithm and returns all randomized data to the query plan executor. The query plan executor executes the Integrate Algorithm on all returned data to execute the outputs the result of user’s request. The data is cryptographically encrypted and decrypted to preserve privacy.

Index Terms— Privacy management, Security policy integration, Conflict reconciliation, Similarity-based policy.

CONCLUSION

In this paper, we have presented an approach to security policy integration and conflict reconciliation for collaborations among organizations in ubiquitous computing environments. Based on the similarities between security policies, a resource owner can adapt its existing security policies to cover the new users from collaborating organizations using the similarity indices as a selection criterion for selecting similar policies in the collaborating organization and make a decision based on their inputs.

FUTURE SCOPE

We plan to conduct case studies to establish some applicable guidelines for specifying the similarity threshold and updating the confidence weight in the decision making process. In addition, we will investigate the impact of extending the security policy set through logical reasoning and try to associate that impact with policy similarity so that we can update the resource owner’s security policies based on the similarity analysis, rather than relying on similar security policies specified by the collaborating organizations. This approach can be further applied to a distributed structure.

REFERENCES