Name of the Scholar: Dharmender
Name of the Supervisor: Prof. M.N. Doja
Department: Computer Engineering
Title of Thesis: SECURITY PROTOCOLS: A NEW APPROACH

Abstract

Authentication is a procedure to verify that received message came from the alleged source and has not been altered. At best, authentication verifies that the received document came from the claimed network source. It cannot verify that the document complied with all the rules and procedure required by the source enterprise. In all commercial and business applications, the documents need to be authorized to bind the document legally with the originating enterprise and authenticated as well. Authorization at source refers to the internal process of an enterprise where by a document is created and processed before transmission to the receiver. In authorization the document is checked whether it is according to authorization rules of the organization or not. A document, which has been authorized at source, is legally enforceable and receiver would expect it to be honored by the originating enterprise.

On receipt of a document, the process that the recipient enterprise carries to ensure that the documents was prepared in accordance with all relevant rules and regulation of the originating enterprise is referred as verification of authorization at source. In all these cases, however, the disclosure of information about the sender enterprise remains a source of concern. In many situations, however the need arises to verify the authorization at receiver

end without the help of sender and without revealing the internal structure of the sender enterprise.

To achieve the above mentioned objective, in this these, we have presented a scheme of providing authorization of an electronic document with the following ideas:

1. XML policies are used for authorizing XML document.
2. XML policies are attached to the XML document and they further help in verification of authorization at receiver end.
3. Where a person in an organization has multiple authorities to exercise, these authorities interact when the person is dealing with an organization to finalize a deal.
4. Implement a scheme in the industrial environment enabling authorized SCADA commands which provides security, confidentiality, and integrity to SCADA communication in controlling a plant at remote site.
5. Implementation of a queuing model for hierarchical setup of an organization. How authorities of a person change in an organization when he joins an organization, he gets promotion, and may leave the organization. The queuing model presented here studies his waiting time service time etc.