DIGITALISED INFORMATION SECURITY IN DATA COMMUNICATION

Elakkiya J, Assistant Professor,
Shrilekha D P, Swathi R
Final Year
Information Technology Department, St. Joseph College of Engineering, Chennai.

ABSTRACT:

In cyber physical systems integrations, the request from the local servers will be processed remotely and the data needs to be model mapped. So that, no one can distract the data and its transfer. Inter-organizational process systems play a very important fundamental role in business relationships. We introduce the concept of *organisation Behaviour.* Not only canthese authentication will be used to ensure authenticity but also it protect integrity of conceptual process data, but also to prove the sequence and logical relationships, such as AND-join(Combination of Data Models) and AND-split, of a conceptual process. A multi-Level validation of data is done through multi key verification token binding on the messages. This will create a highly secure and competitive strength to the system. A multi-Level validation of data is done through multi key verification token binding on the messages. This will create a highly secure and competitive strength to the system.

1.INTRODUCTION:

In today's business world, forming an alliance with appropriate business partners is a common strategy for an enterprise to stay competitive by offering a wider range of products and servicesto its customers with the advancement of service-oriented computing, particularly cloud computing, it is also becoming a norm for enterprises to outsource parts of their business processes to a third-party service provider. This way, the enterprises can focus on their core competencies, while improving the speed and quality of their business processes and reducing the business cost. Hence inter-organizational (or cross-organizational) conceptual process management systems, for example ERP , SCM and Crossflow , play a very important role in executing business processes among business partners or outsourcers/outsources in a dynamic and timely manner. Briefly, an inter-organizational conceptual process management system is used to model and control the execution of

business processes involving a combination of manual and automated activities between organizations. Henceforth, we consider only decentralized, inter-organizational conceptual process systems.

2.LITERATURE SURVEY:

Mediated cipher text-policy attribute-based encryption and its application. In Cipher text-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the cipher text is associated with an access policy over attributes. The user can decrypt the cipher text if and only if the attribute set of his secret key satisfies the access policy specified in the cipher text. Several CP-ABE schemes have been proposed, however, some practical problems, such as attribute revocation, still needs to be addressed. In this paper, we propose a mediated Cipher text-Policy Attribute-Based Encryption (MCPc-ABE) which extends CP-ABE with instantaneous attribute revocation. Furthermore, we demonstrate how to apply the proposed MCPc-ABE scheme to securely manage Personal Health Records (PHRs)

Identity-based encryption (IBE) is an exciting alternative to public-key encryption, as IBE eliminates the need for a Public Key Infrastructure (PKI). The senders use an IBE do not need to look up the public keys and the corresponding certificates of the receivers, the identities (e.g., emails or IP addresses) of the latter are sufficient to encrypt. Any setting, PKI- or identity-based, must provide a means to revoke users from the system. Efficient revocation is a well-studied problem in the traditional PKI setting.

However, in the setting of IBE, there has been little work on studying the revocation mechanisms. The most practical solution requires the senders to also use time periods when encrypting, and all the receivers (regardless of whether their keys have been compromised or not) to update their private keys regularly by contacting the trusted authority.

3.SYSTEM DESIGN:

System Design involves identification of classes their relationship as well as their collaboration. In objector, classes are divided into entity y classes and control classes. The Computer Aided Software Engineering (CASE) tools that are available commercially do not provide any assistance in this transition. CASE tools take advantage of Meta modelling that is helpful only after the construction of the class diagram. In the FUSION method some object-

oriented approach likes Object Modelling Technique (OMT), Classes, and Responsibilities. Collaborators (CRC), etc, are used. Objector used the term" agents" to represent some of the hardware and software system. In Fusion method, there is no requirement phase, where a user will supply the initial requirement document. Any software project is worked out by both the analyst and the designer. The analyst creates the user case diagram. The designer creates the class diagram. But the designer can do this only after the analyst creates the use case diagram. Once the design is over, it is essential to decide which software is suitable for the application.

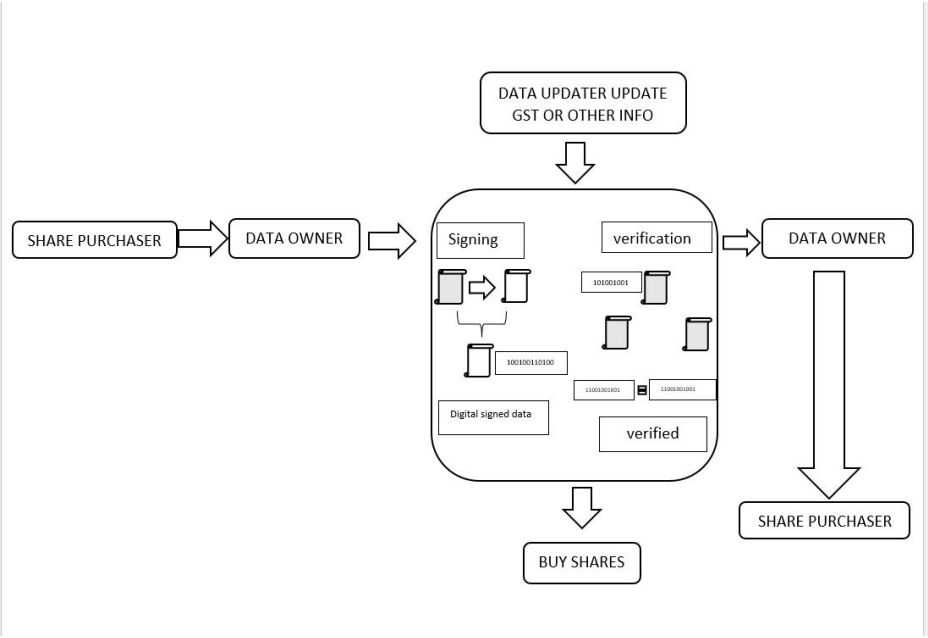

FIGURE 3.1 SYSTEM ARCHITECTURE

4.IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Authentication Module describes the interface between the user and system and the admin provided the type of authentication. The user is allowed to create his credentials to login into the system. An admin needs to approve the users created and login approval the user will be allowed to access the application. Authentication is provided by encrypting the username and password. Protecting sensitive information from users. This can be achieved with the help of SHA1 algorithm. SHA1 is cryptographic hash function. The Application configuration file is loaded with MD5 based encryption algorithm. So that, the user doesn't have clear connection string into their application configuration file. Using this, the configuration information related to the server is hided from the users or intruders. Triple DES encryption is used to encrypt owner's data. The owner going to send data to third

party(data updater) before sending data to third party ,the owner digitally sign data , which is in XML format.

5.CONCLUSION AND FUTURE ENHANCEMENT:

Once the verification token on the message is obtained from the Signing Authority and some system parameters (fixed and published by the PKG). This message will be sent to the destination and in the destination point the verification token will be validated with the basic identifier and system parameters known by the destination person. Identity Based Verification token (IBS) scheme involves various steps like setting up the master keys, Extracting the private key from the master keys, Signing the message with the obtained verification token, and verifying the verification token in the destination. Everything is automated through a sequence of workflows. In the multilevel of workflow, the verification token will be amended with multiple approvals which in turn provides the strongest way of auditing and authenticating the data.

6.REFERENCES:

[1] W. Bartschat, J. Barrington-Brown, S. Carey, J. Chen, S.Deming, and S. Durkin, "Surveying the RHIO landscape: A description of current {RHIO} models, with a focus on patient identification," *J. AHIMA,*vol. 77, pp. 64A–64D, Jan. 2006.

[2] A. P. Sheath and J. A. Larson, "Federated database systems for managing distributed, heterogeneous, and autonomous databases," *ACM Compute Surveys (CSUR), vol. 22, no. 3, pp. 183–236, 1990.*

[3] L. M.Haas, E. T. Lin, and M.A. Roth, "Data integration through database federation," *IBM Syst. J., vol. 41, no. 4, pp. 578–596, 2002.*

[4] X. Zhang, J. Liu, B. Li, and T.-S. P. Yum, "CoolStreaming/DOT Net: A data-driven overlay network for efficient live media streaming," in *Proc. IEEE INFOCOM,Miami, FL, USA, 2005, vol. 3, pp. 2102–2111.*

[5] A. C. Snoeren, K. Conley, and D. K. Gifford, "Mesh-based content routing using XML," in *Proc. SOSP, 2001, pp. 160–173.*