

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology



ISSN 2320-088X

International Conference on Mobility in Computing- ICMiC13, Organized by Mar Baselios College of Engineering and Technology during December 17-18, 2013 at Trivandrum, Kerala, India, pg.114 – 118

SURVEY ARTICLE

A Study of Work Flow Domain Authentication

Anu Aravind¹, Anitha Sandeep²

Department of Computer Science & Engineering, Mar Baselios College of Engineering, Kerala University, India

¹ anrajcse@gmail.com; ² anitha.sandeep@gmail.com

Abstract—*The workflow scheme plays a vital role in the development of business partnerships. Different organizations are included in this cross-organizational work flow. The workflow structure uses the business cases which enables the business integration. To carry out the processes, different security measures have to be imparted which set off workflow signature throughout each task. It provide commercial work flow management platform and provide more importance to the ERP management.*

Keywords— *Cross organizational; Digital Signature; Cryptography; Authentication; Cloud Computing*

I. Introduction

In this business world forming a coalition with the business partners is a very common strategy. With the arrival of service –oriented computing particularly the cloud computing, it becomes much easier for a third party alliance. This enables the speed and accuracy of the inter operability of an enterprise. The application of work flow management system is widely spread. Initially the emphasis of work flow management was inside the organization. Later on it developed to the inter-organizational structure. This linked work flow system allows, one process flow of an organization to make use of another process of different organization and thus increase their speed of work. In cloud computing, a large number of computers connected through a real time communication network. The main advantage of cloud computing is that it does not require very high capital. It consists of services of both hardware oriented and software oriented. These services are referred to as software as service. The data-center represented in hardware and software is generally known as cloud. The cloud can be represented as public cloud and private cloud. When the cloud becomes payable it is generally called as public cloud. When it becomes internal characterization with in business organization it is called private cloud. The cloud computing enables the long dreamed vision of computing ability. As an advantage, a large number of data centres with low cost can be modelled. As a result the resources become available in pay-use model and provide multiplexing among a large group of customers.

In the cross-organizational workflow, an organization mainly focuses on their core area of business and provides an arrangement to contract out their secondary activities to other organizations. As a result there is a tight collaboration between these organizations. Once an infrastructure is maintained there is a need to maintain a link between them. But outsourcing of the data need to be automated and must be done under various security measures. Each task should be done with the authenticity, managing the process in an individual organization.

The workflow scheme has developed for the integration between various organizations. There must be well established structure for the entire process to be manifested. The scheme has initiated with various methods that

work on processes. Later, added with more powerful cryptographic algorithms, bring more strength to the structure.

II. The Related Work

A. THE WORKFLOW MANAGEMENT COALITION[2]

It studies the objectives of advancing and exploitation of work flow technology. It identifies a path to incorporate the essential and more required security services. For a work flow system to establish, it requires several security provisions which merely depend on the underlying software architecture. It basically concentrates on the work flow inter-operability. The security measures over a workflow depend on the underlying cryptographic algorithms. More security services can be provided if the algorithm is strong. While considering the security, the main factors related are authentication, authorization, data integrity, access control, audit and data privacy. *Authentication* is the act of confirming the truth of an attribute of a datum or entity. The main context of work flow is authentication, in which the administrator can perform the log-on activity within a workflow service. *Authorization* is a function of specifying access to the resources which is related to information security and computer security in order to provide the access control. In workflow service, interoperability occurs in 2 or more different domains. Thus the role based depends heavily on user authentication and authorization in each work flow domain. *Access Control* is a practice of providing restriction at entrance, i.e., it provides access only to the authorized persons. In the case of work flow, it may operate on the log-on and to access the particular activities. *Data Privacy* refers, whatever data is transferred between two parties, it will be secured and will not be interpreted by a third party. In a workflow scheme it is important to provide the confidentiality between the data transferred and it is normally provided by the cryptographic algorithm. *Data Integrity* provides assurance that whatever data is transmitted between the parties it will not be altered. In workflow process the data integrity is necessary since the data is operated between various domains. So the data integrity and data privacy are the important factors related to workflow scheme.

B. CROSS-ORGANIZATIONAL WORKFLOW MANAGEMENT IN DYNAMIC VIRTUAL ENTERPRISES [3]

It gives a well defined overview about conceptual and technical level in cross flow project. This ropes the cross organizational workflow management development. It aims for the end-end solution which comprises of all functionality for an outsourcing service. Cross flow is basically a European research project which develops workflow organization for virtual enterprise. There is a cross flow approach which provides an advance support in dynamic virtual organization. On the whole there are 3 aspects which typify the workflow structure. The different phases are *dynamic service outsourcing*, *contract based service specification*, *fine grained advanced integration*. In dynamic service outsourcing, the partners coordinate their process based on outsourcing. If an organization desire to outsource their service, it can farm out to its consumers. The interaction between the providers and consumers are merely based on the contract and the representation of dynamic service outsourcing is shown in Fig 1.

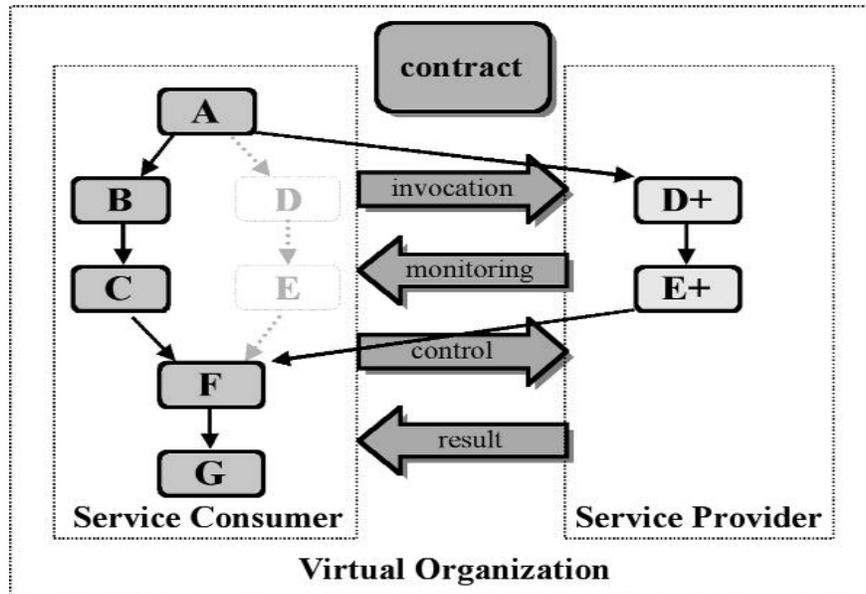


Fig 1: dynamic service outsourcing in virtual organization

In contract based service specification, a contract represents the tightly link between the provider and the consumer. This entails the process which is used to execute the service. In virtual organizations high level of integration is essentially required for the participation. In IT establishment different platforms exist which leads to a heterogeneous environment. The cross flow systems exist between the organizations on the basis of abstraction level and fine grained advanced integration and the interaction between the consumer and customer must be of fine grained level. To provide a tight bound between the processes, a notion of interactions is required. Based on this context the various sub process are interacted and they can be combined to generate a reformed work flow scheme. In generally these three areas are taken in to provide a quality of service to the third party participant who basically focuses on the cross-organizational workflow in a virtual environment.

C. SECURE WEB SERVICE WORKFLOW EXECUTION [4]

It props up the automated implementation of business courses. Here the workflow is defined as interrelation of web services, participates in the process, instruct the communication between the processes. There are two different interaction between single web services one is termed as service orchestration which refers to the centralized service request-reply transformations and other is service choreography in which multiple engines performs request-reply at different locations. In the automation of a business course information is passed from one member to another based on a set of system convention. To ensure the framework the security policies uses the Public Key Infrastructure which generates the public key and private key certificates for the deployment of work flow. The layout of the workflow description is represented in Fig 2.

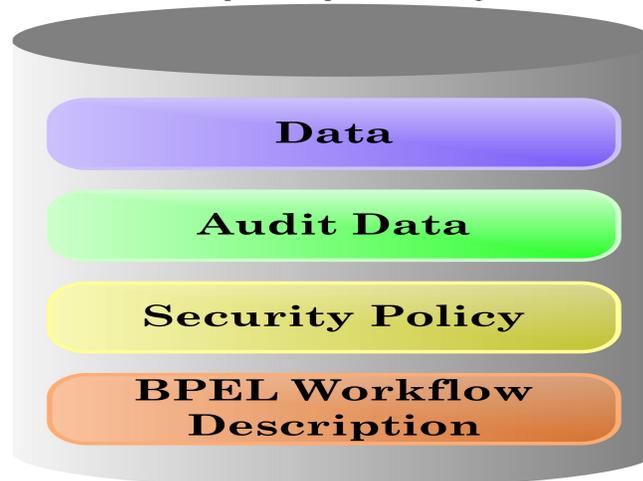


Fig 2: Process Slip

The data is a storage place where the input data is shifted among successive process. Security methods are added to safeguard integrity. Encrypted data are accessed by means of tickets issued by PKI. In audit data, each concerned manager write the log data which specifies about request partner, request operation, request assignment. Security policies spell out security boundaries for each and every pace in the work process. The entire procedure is inhibited by a workflow depiction. This inert data structure will not be transformed during the implementation of the workflow and only mention the location about the description. The XML signatures can be used to verify the truthfulness and endorsement.

D. WORK FLOW SIGNATURE FOR BUSINESS PROCESS COMPLAINCE [1]

It proposes more secured features for the cross organizational work flow scheme. Initially the present system was based on the username and password. As an enhancement a digital signature is introduced by considering more security measures. For each task that is generated in this work flow, it requires signing keys to grant permission. This signing key will generate the authorization of the workflow that can be controlled at run time [1]. This work flow scheme generates a digital signature for each task as an authentication which uses the hierarchical identity based cryptography. Basically in inter-organizational workflow systems the fundamental role is business partnerships. To ensure the security, authenticity and integrity the concept of workflow signature has been introduced. The workflow signatures can provide electronic evidence for auditing and it can also be used to grant permission to perform tasks. The general representation of this workflow scheme is represented in Fig 3.

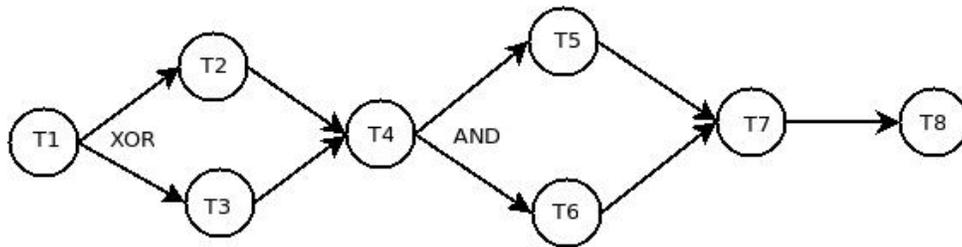


Fig 3: A business travel planning work flow

The workflow signature scheme comprises five algorithms: ROOT SETUP, NEXT-LEVEL SETUP, EXTRACT, SIGN, and VERIFY. The ROOT SETUP can be run by only a trusted Central Workflow Engine, while the other algorithms are run by either the CWE or a task execution agent. The description of the algorithms is explained with ref [1]:

1. Root Setup

This algorithm is performed by the CWE. It generates the system parameters and a master secret on input a security parameter. The system parameters, which include a description of the message space M and the signature space S, will be made publicly available to all execution agents.

2. Next Level Setup

This algorithm allows an execution agent to establish a secret value to be used to issue private keys to the subsequent agents in the workflow.

3. Extract

This algorithm is performed by the CWE or an execution agent with workflow identifiers ID_j where $1 \leq j \leq m$ and t_j denotes the position of the j_{th} workflow identifier in a workflow namespace. The algorithm computes a private key SK_{t_j} for any of the immediate subsequent agents in the workflow using the system parameters, its private keys (corresponding to identifiers ID_{t_j} for $1 \leq j \leq m$) and any other secret information.

4. Sign

Given a set $SK = \{SK_{t_j} | 1 \leq j \leq m\}$ of signing (private) keys, a message $M \in M$, an authenticator set $Auth$ (generated by the next immediate agents in the workflow) and the system parameters, the algorithm outputs a signature.

A workflow signature authenticates a workflow by providing typical conditions related to authenticity and integrity. It can be used as proof for certain regulations and moreover it is a proper verdict for a task based authentication control. It provides an authentication and electronic evidence and can provide grant access permission in a work flow scheme.

III. Discussion and Open Problem

A workflow structure provides technical and conceptual descriptions in cross flow project. Initially this formation was developed for the homogeneous organization. Mostly in homogeneous environment the structure of the workflow will be in a centralized manner. It performs all the centralized actions. But the main drawback of this system is the single point of failure when many associates sharing single system. As a contrast to the centralized system a concept of de-centralized system has been invoked.

The work flow structure grants an advance support for the dynamic virtual organization. An organization can outsource their business activities only through a secure manner. The security basically relies on the underlying cryptographic algorithms. Widely accepted form was to use the Public key Infrastructure which comprises of public key and private key. Many amendment forms have been generated for the transformation of the data between various domains. One such process is the digital signature development, which impart the authentication through system generated mode. Digital signature appears to be an improved form in a de-centralized environment. It can provide an advance authentication technique along with integrity. Digital signature can be used as an electronic confirmation. This approach fits well in task based authentication. However a major problem to the digital signature in work flow is that, each time the signature generated is of varying length and makes the entire structure a more complex one. As a solution to this problem, it will be efficient to generate the signature of constant –length.

IV. Conclusion

This work flow authentication specifies the emerging of workflow structure from its initial security measures to the wide developed digital signature implementation. At each phase, the work flow structure explains its operability to the both consumer and participant. In a decentralized system the whole system relies on the underlying security measures. Initially it uses the scheme of PKI interface and currently updated with the digital signature creation on each task –task communication. This digital signature verifies the authenticity of the sender. As a superior to the above procedure, a timestamp can be added to each verification such that when the timer expires the task can regenerates the communication. However the problem of variable length signature is still opened for more research work.

References

- [1] Hoon Wei Lim, Florian Kerschbaum and Huaxiong Wang “Workflow Signatures for Business Process Compliance”, IEEE Transactions on Dependable And Secure Computing Vol 9 No 5, September/October 2012
- [2] The Workflow Management Coalition Specification Document Number WFMC-TC-1019 Document Status Issue 1.0 Feb 98
- [3] Paul Grefen, Karl Aberer†, Yigal Hoffner‡ and Heiko Ludwig,” CrossFlow: cross- organizational workflow management in dynamic virtual enterprises” vol 15, September 2000
- [4] Carsten Rudolph, Nicolai Kuntze, Zaharina Velikova,” Secure Web Service Workflow Execution”, 2007
- [5] S. Eckartz, M. Daneva, R. Wieringa, and J.V. Hillegersberg, “Cross-Organizational ERP Management: How to Create a Successful Business Case?” Proc. ACM Symp. Applied Computing, S. Shin, and S. Ossowski, eds., pp. 1599-1604, Mar. 2009
- [6] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia,” Above the Clouds: A Berkeley View of Cloud Computing” , February 10, 2009
- [7] Rajkumar Buyya^{1,2}, Chee Shin Yeo¹, Srikumar Venugopal¹, James Broberg¹, and Ivona Brandic³,” Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility”, 2008