IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VII (Sep – Oct. 2014), PP 01-07
www.iosrjournals.org

A Flexible Method Using Identity Based Message Key Distribution for Securing Workflow Signatures

Roshin Sharo Eapen
Dept. of Computer Science and Engineering, Mahatma Gandhi University, India

Abstract: *The increase in advancement of information technology led the migration of workflows from paper based to electronic workflow systems. Basically a workflow consists of a number of tasks and each of these tasks should be authenticated by using any of the cryptographic techniques. To provide more security within workflow systems, signing keys are used. In addition to data authenticity and integrity, logical relationships such as AND-join and AND-split are to be provided in a workflow signature scheme. Such a scheme was experimentally proven which is based on hierarchical identity-based cryptography to meet security properties required by inter-organizational workflows. Due its high complexity, a new mechanism, IB-MKD (Identity Based Message Key Distribution) is proposed as an alternative to HIBS, which is achieved with conventional RSA without any additional assumptions and limitations and it is believed to have less overhead.*

Keywords: *Business processes, central workflow engine, cryptography, digital signatures, workflow.*

I. Introduction

In today's fast changing competitive business environment, organizations are continually driven to develop their new marketing strategies.A strategic alliance can be defined as an agreement between two or more organizations to achieve more benefits and to gain competitive advantage. Forming an alliance with appropriate business partners is becoming a common strategy for an enterprise to stay competitive in the marketing field. In simple words, it is sometimes referred to as a partnership that promotes mutual beneficial opportunities. With the increase in advancement of cloud computing[1], enterprises began to outsource their products to a third-party service provider. The number of third party service providers began to rise offering an ever increasing number of services as the companies saw the benefits of outsourcing delivery functions. This way, an enterprise can improve the speed as well as quality of the business processes by focusing on the core competencies among various organizations and thus they can reduce overall business cost. And this is whythe inter-organizational workflows such as ERP[2], SCM[3] and Cross Flow[4]play a vital role in running business process executions in a dynamic and timely manner.Briefly a cross organizational workflow management system controls and models the manual as well as automated activities between organizations[5].A workflow can be defined as the automation of a business process in which various tasks are passed from one participant to another as per a set of rules. Basically a workflow may consist of a number of tasks and each of these tasks should be authenticated by using any of the cryptographic techniques. With this context, a workflow management system defines, creates and manages the execution of workflow. In a workflow system, the workflow management engine can be either centralized or decentralized. In a centralized workflow system, the central workflow engine (CWE) is responsible for distributing the related task to the appropriate task agent in a workflow whereas in a decentralized workflow system, the central workflow engine sends the entire task to the first execution agent in the workflow and this will be received as the final output from the last execution agent in the workflow system.Mostly the latter one is preferred than the former due to scalability and heterogeneous and autonomous nature of organizations.

The development of the technologies led the migration of paper based systems to electronic workflow systems. Paper based workflow signatures are used for different purposes such as authorization, accountability, authentication etc. With the changing world, organizations move away from paper documents with ink signatures or authenticity stamps to digital signatures as they can provide added assurances that the message is from the claimed sender. In the electronic world, the evidence can be only be generated by the correct signer by some mathematical computation. This result we got after the computation is generally termed as a digital signature. Public key cryptographic scheme is a common method to compute digital signatures. Standard public key cryptographic schemes that have been used to implement signatures are Rivest-Shamir-Adleman (RSA) scheme and Digital Signature Algorithm (DSA) scheme. In these schemes, a key-pair containing a private keyand a corresponding public key is owned by a user. The private key is meant to be only knownby the owner, and the public key is known to the public. The mathematical properties of the public key system ensures that a message i.e.,the plaintext, after encrypting with a private key only known by the user and then decrypting with the corresponding public key will become the plaintext itself. And at any cost, there will be no computationally feasible way to computethe corresponding private key with a given public key.

In this paper, the use of digital signatures in workflow systems and their roles in business process executions is introduced. In a distributed environment, digital signatures seem to be a better choice for workflow signatures rather than classic/password authentication mechanisms even though they are commonly used. In addition to data authenticity, cryptographicallysecure signature schemes can be usedto protect data integrity of a workflow.For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver the reason to believe that the message was sent by the claimed sender. Furthermore, digital signatures can also serve as electronic evidence for the purpose of auditing. A digitally signed event messages related to tasks within a workflow serve as proofs that the associatedbusiness processes have been taken place and authorized by therelevant parties. Such a scheme was experimentally proven which is based on hierarchical identity-based signature(HIBS) scheme[6],[7] to meet security properties required by the inter-organizational workflows but its implementation is a bit complex. So a new mechanism, IB-MKD (Identity Based Message Key Distribution) is proposed as an alternative to HIBS which is achieved with conventional RSA without any additional assumptions and limitations and it is believed to have less overhead and more secure.

In the following section, some basic concepts of inter-organizational workflows are described. Section 3 describes the related work in literature. Subsequently proposed workflow signature scheme is presented in section 4. In the next section, a study of comparison of trust assumptions is made. Then in section 6, a system analysis is done and finally section 7 concludes my work.

II. Related Work

As we all know that an ink signature could be generated from one document to another by copying the image manually or digitally. To have credible signature copies that can resist some scrutiny is a significant manual or technical skill, and alsoto produce ink signature copies that resist professional scrutiny is very difficult. Digital signatures bind an electronic identity to an electronic document cryptographically and the digital signatures cannot be copied to another document. There seems to be only a relatively small amount of work thatexamines basic security issues of workflow systems, particularly in terms of authenticity and integrity protectionof workflow information and sequence. Most of the security related existing works in workflow systems usually assume the existence of the appropriate complementary security mechanisms and infrastructures that can prove authenticity and integrity of workflow information. And they may also focus on various access control aspects of workflow systems, such asaccess control modeling, temporal authorization, workflow constraints.

Montagut and Molva investigated the traceability andintegrity aspects of the decentralized interorganizational workflow executions[8]. They proposed the use of onion encryption[9] and standard signatures to ensure that cryptographic keys can be accessed only during execution of the relevant tasks, and thus proved that the integrity of a workflow sequence and its associated data are protected. With their investigations, they assumedthat each execution agent within a workflow isassociated with a policy-based key pair[10] which is then often used to distribute task-based cryptographic keys which in turn, are used by execution agents for signing workflow information and task related data. Each of these task-based keys is encrypted using policy-based public keys and onion encryption techniquesto form an “onion.” The onion is then forwarded with other associated workflow data is then forwarded to the agents. Only an authorized agent would be able to access to the appropriatetask-based keys using the correct policy-based private keyby “peeling off” a layer of the onion.

In a Chinese wall security model proposed by V. Atluri, S. Chun, and P. Mazzoleni for the decentralized workflow management system[11]solvesthe conflict of interest in the self describing workflow. The company datasets are represented as disjoint conflict of interest (COI). For example, Banks, Oil Companies, Air Lines are the different conflict-of-interest classes. This policy ensures the prevention of information flow from one company to another that cause conflict of interest for individual consultants. Even though these techniques are interesting, they are too inflexible to be practically feasible. Although the associated execution agents can be selected at runtime, a workflow sequence is static because task-related keys must be precomputed during initialization of the workflow. This implies that for a workflow containing AND/OR-join/split relations, the workflow initiator must consider all possible branches of the workflow and thus, compute an onion reflecting all possibilities. Also Hoon Wei Lim, Florian Kerschbaum, and Huaxiong Wang proposed workflow signature scheme for secure business process compliance and the work was experimentally proven too[12]. They proposed a concrete workflow signature scheme, which is based on hierarchical identity-based cryptography, to meet security properties required by inter-organizational workflows. But the method is a bit complex.The proposed work is somewhat related to, but different from the above work. Instead of using HIBS,IB-MKD is proposed in the new work and it is used with conventional RSA without any additional assumptions and limitations. The proposed work uses a centralized approach with the workflow agents. This work also ensures less overhead and low cost with more privacy.

III. Inter-organizational Workflows

Inter-organizational workflows offer companies to reshape the scope of business processes beyond individual organizations. It improves the effectiveness and efficiency of business process within an organization. Inter-organizational workflows support the cooperation and communication of different autonomous entities such as companies or organizations. Workflow is the automation of a business process in which tasks are passed from one participant to another according to a set of procedural rules. A participant may be a person or an automated process or a local or in a separate remote organization. A business workflow is a collection of well-defined tasks and the associated task dependencies control the coordination among these tasks. Each task in a workflow corresponds to the associated task execution agent. We denote a task as ti, and its execution agent as A(ti). In a decentralized, inter organizational workflow, execution agents are usually different that the evaluations of task dependencies are performed by the agents without relying on a central workflow engine. Here an example of inter-organizational workflow is illustrated.Let us now consider an example of a business travel planning process. As a part of this process we need to book a flight ticket, a hotel room and car reservations through an agency. Graphical representation of the workflow is represented in Fig. 1 and the associated tasks are as follows.

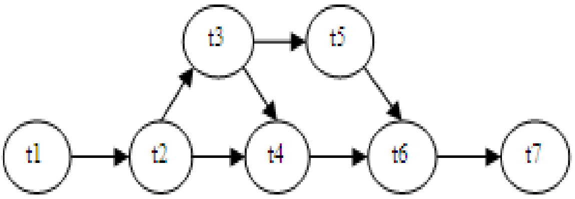

Fig. 1 A business travel planning workflow

The above workflow depicts the following tasks.

- t1: Input the travel information;
- t2: Request for a flight ticket from Indigo airlines;
- t3: If t2 fails or if the ticket costs more than $500, then reserve a flight ticket from Delta airlines;
- t4: If the ticket at Indigo airlines costs less than $500, or the reservation in Delta airlines fail, then purchase the tickets from Indigo;
- t5: If delta has a ticket, then purchase it from Delta;
- t6: Reserve a room from Hotel Booker; and
- t7: Rent a car at Ace.

Assume that each task is well executed at its appropriate agent for example, the task t2 is executed by the agent Indigo airlines and the task t3 is executed by the agent Delta airlines. In our example workflow of a traveling process , A(t1) is a travel requester who needs to perform task t1, that is to input the travel information into the workflow system. After the completion of task t1, agent A(t1) forwards the remaining workflow (t2; . . . ; t7) to the next agent A(t2), a travel agency named Indigo airlines. Agent A(t2) is then expected to execute task t2 and send the remaining workflow (t4; . . . ; t7) to agent A(t4). In addition, agent A(t2) triggers the execution of task t3 by agent A(t3), another independent travel agency named Delta airlines in parallel, as part of the company travel policy, for example. As per the entered information if the outcome of t2 results more than $500 or if the task t2 fails, then the ticket is to be booked from the other agency i.e., Delta. Next, agent A(t4) then purchases the tickets from Indigo, if the ticket at Indigo airlines costs less than $500, or the reservation in Delta airlines fails. Else the next agent A(t5) is executed by purchasing the ticket if Delta has one. In other words, agent A(t4) or A(t3) would forward tasks A(t6). Subsequently, agent A(6), followed by agent A(7), execute their respective tasks. At the end, agent A(7) reports the results back to the central workflow engine.

IV. Proposed Method

In order to avoid the complexity in the existing approach, a new scheme based on IB-MKD is proposed which maintains a centralized approach. In an inter-organizational workflow management system, we assume that there is a CWE which acts as a central management system accessible by other agents or business partners. There is no workflow complexity to the task agents as the workflow is maintained by the CWE only. The role of the CWE is to initiate a workflow which is to be sent to the appropriate first execution agent. Only the CWE has the entire workflow plan with it and when the first execution agent is invoked, it sends a request with its ID. Then the CWE passes the corresponding data to the agent. And the process continues, finally output of the workflow is then sent to the CWE by the last execution agent in the workflow.We assume that task related information is communicated between two workflow stubs. This workflow may contain information such as:

- A CWE with the entire workflow,
- The task execution agents A(ti) with its parameters.

Meanwhile, a workflow stub is a small component attached to a task execution agent which helps in communicating with the CWE and forwards each self-describing workflow to the relevant agent. We envision that a workflow stub alsoperformsall cryptographic operations involved during the execution of a task.

4. 1 Architectural Overview

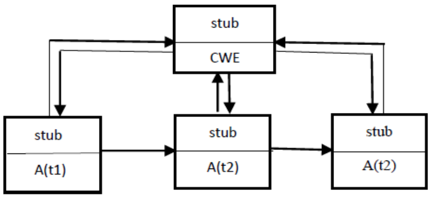

Fig. 2 Framework for securing inter-organizational workflow system

As already mentioned, the CWE only has the entire workflow to be executed. Each of the work in a workflow has IDs. Initially, all the task execution agents including CWE generate its system parameters (PK, SK) i.e., public key and secret key and each of the agents will be having their own IDs. After that the public keys of the execution agents will be made available to the CWE. Then CWE calls the first execution agent in the workflow using a method. Once the first execution agent say, A(t1) is called, it sends a request with its ID to the CWE to start the workflow.

$$A(t1) \xrightarrow{ID_{A(t1)}} CWE$$

On receiving the request, CWE replies A(t1) with its public key, workflow ID, recipient ID and recipient public key. Here the recipient is A(t2).

$$CWE \xrightarrow{PK_{CWE},\ ID_{WF},\ PK_{A(t2)}} A(t1)$$

After getting all these details, A(t1) with its unique key ‘k’, encrypts the data which is to be send to the next agent. Then it encrypts ‘k’ with the recipient ID. And it binds it with a signature that has been encrypted with the secret key of the sender A(t1). Finally the encrypted data, encrypted unique key, encrypted signature, recipient ID and workflow ID is as a whole encrypted with PK_{CWE} and this is finally sent to the receiver.

$$A(t1) \xrightarrow{E(m)} A(t2)$$

Where, $E(m) = \{\{m\}k,\{k\}PK_{A(t2)}||\{S\}SK_{A(t1)}||IDR||ID_{WF}\ \}PK_{CWE}$

When the receiver receives the message E(m), it keeps the first part, i.e., the message encrypted with the unique key of the sender while the second part is sent to the CWE.CWE then decrypts the second part with its private key as it is encrypted using its public key by the sender. After decrypting, it obtains the IDWF and IDR. It then verifies the signature of the sender using sender’s public key and if it finds that it is from an authorized sender, and then the decrypted part will be send to the receiver. As the unique key ‘k’ of the sender is encrypted by with the recipient’s public key, the receiver decrypts it using its private key. After knowing the private key of the sender, the receiver decrypts the message send by the sender using ‘k’. Again the process of workflow continues by the CWE invoking the next agent in the workflow and sending its public key. If there are two agents showing an ‘AND ‘relation, then the public keys are send to both the agents simultaneously. Then the process continues and finally it reaches the last agent. When the final agent say, A(tn) decrypts the message, it is then send back to the CWE. For the symmetric encryption standard scheme AES is used, and for the asymmetric encryption RSA is used.

4.2 Workflow Signatures

A workflow signature proves the security of a workflow to a business process model. A business process model contains a directed graph of vertices or tasks denoted by ‘ti’ and edges or task dependencies denoted as 'ti-tj'. Each vertex with two or more outgoing edges is called a split and each vertex with two or more incoming edges is called a join. Both split and join is associated with a specific type {AND;OR;XOR}. Edges are executed in parallel in an AND-split. Only one edge can be executed in an XOR-split, and in an OR-split at least one edge is executed.

4.3 Encryptions Used

For encrypting the data or message which is to be transferred between the agents in a workflow and the signature encryption techniques RSA and AES are used respectively.

4.3.1 RSA: It is an asymmetric encryption and authentication system that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman IN 1977. It is the most commonly used encryption and authentication algorithm. The encryption system is owned by RSA Security. Briefly, the algorithm involves multiplying two large prime and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key.

4.3.2 AES: The Advanced Encryption Standard (AES) is based on a design principle known as a substitution-permutation network combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.

V. Comparison Of Trust Assumptions

While choosing any security system, we must recognize and accept the associated trust assumptions also. As told earlier, our system hasn't got any additional assumptions than that of the existing system that uses Hierarchical Identity based Scheme (HIBS). But they require somewhat stronger assumptions than RSA. Apart from these assumptions, a number of benefits can also be achieved. Following are the assumptions made in the system.

Practical deployment of IBE and/or RSArequires domain-based administration where each domain managesits own PKG or CA(Certificate Authority). In our workflow system, CA is central workflow engine(CWE). In both cases, the sender must obtain the PKG public keyor the CA certificate for the recipient's domain that allows it to determine the public key of the recipient. This enables the sender to compute the public key in IBE whereas in RSA, this enables the sender to lookup the recipient'scertificate in a directory to verify the CA's signature on the certificate and to obtain the recipient's public key. In this aspect, IBE and RSA have similar trustassumptions. We must also trust that the PKG/CA private key is known only to itself. Compromise of the PKG private key compromises the private keys of all users in that domain. On the other hand, compromise of the CA private key enables the attacker to sign and publish new compromised public keys, make the senders encrypt new messages to these public keysBut here this risk is addressed by keepingthe CA private key offline so it is not subject to online attacks. But to keep the PKG offline is feasible only if long-lived keys are used. However, IBE must use short-lived keys to support revocation. So, in practice, the PKG must remain online, with the associated increased risk of compromise.Thus, in this aspect, IBE requires stronger trust assumptions than RSA. We also require a trustworthy process by which recipients obtain and manage their private keys. Also in IBE, the PKG generates the private keyand sends it to the recipient through a private, authenticated channel. Thus, in both cases, wemust trust the user authentication to the PKG or CA, so private keys are not associatedwith the wrong recipients. However, we must also trust that the private key is not compromised at the PKG or on the network in IBE. Again, IBE requires stronger trustassumptions than RSA.

VI. System Analysis And Evaluation

Our proposed system uses an encryption scheme which is different from the previous approaches. Even though the trust assumptions made are the same it is seen that the previous one uses strong assumption than ours. In fact, there are some practical benefits that can be achieved with our scheme. Apart from that, this section also describes some of the RSA based alternatives to IBE.

5.1 Benefits

Our very simple approach of using IB-MKD achieves all the practical benefits of IBE. They are:

- Eliminates user key distribution as the sender only needs the public key of the CWE to send a message to any recipient.
- Provides policy based encryption as an arbitrary policy can be associated with the encrypted message.
- Provides implicit client mobility as the recipient can contact theCWE to obtain the message key for message decryption from any location.

Furthermore, IBE provides a weaker form of end-to-end security for encryption thantraditional RSA-based PKIs, with the PKG as a possible man-in-the-middle.

5.2 RSA Based Alternatives

A major difference between IB-MKD and other approaches including IBE, IB-mRSA and Callas's approach is that in our solution the sender encrypts the message with domain's (CWE) public key instead of a specific user's public key. A second difference between IB-MKD and IBE is that the former encrypts the messagepolicy (with PK_{CWE}) while IBE does not. This provides more security. Another difference between IB-MKD and IBE is that in IB-MKD the recipient has to contact the CWE for every message rather than once per policy duration as in IBE. However, it is believed that the load imposed here is reasonable.

5.3 System Comparison

A comparison of the differences between proposed solution and four others, namely, IBE, S/MIME, IB-mRSA and Callas is summarized in the table below. An evaluation of these schemes against the trust assumptions and unique benefits is made here. And this evaluation shows that our scheme, IB-MKD achieves all the benefits of IBE without any additional trust assumptions while all other schemes fail to do so.

For the purpose of trust assumptions the entities that are fully trusted by eachscheme and whether or not the schemes provide strong end-to-end security guarantees for encryption are identified here. The ability to eliminate the user key distribution for the unique benefits is evaluated first. They include, how many keys the sender needs to fetch for encryption and how many keys the recipient needs to fetch for supported. The benefits of policy based encryption and client mobility is then evaluated. An additional evaluation parameter is the target encryption key that illustrates a unique feature of IB-MKD.

Table 1 System Comparison

	S/MIME	IBE	IB-mRSA	Callas	IB-MKD
TrustedEntities	CA is partially trusted for publickey distribution.	PKG is fullytrusted.	CA and SEM are fullytrusted.	PKG is fullytrusted.	KDC is fullytrusted.
End-to-endEncryption	CA can't decryptmessages.	PKG candecrypt messages.	CA can decrypt messages butSEM cannot.	PKG candecrypt messages.	KDC candecrypt messages.
Encryption Key fetch	One key fetchper recipient.	One key fetchper domain.	One key fetchper domain.	One key fetchper recipient.	One key fetchper domain.
Decryption Key fetch	Offline. Recipient generates the private key.	One key fetch per policy.	Contact SEMfor partialdecryption of each message.	One key fetch per policy.	Obtain symmetric Keyfrom KDC for each message.
Revocation	OCSP/CRLs.	Short-livedkeys.	Immediaterevocation viaSEM.	Could support short-livedkeys.	Immediaterevocation viaKDC.
Policy-based Encryption	No direct support.	Policy included in keygeneration.	No direct support.	Could be extended to support.	Policy associated with messagekey.
Recipient Mobility	Requires smartcard or keyrepository.	Implicit. Recipient Fetcheskey from PKG.	Requires smartcard or keyrepository.	Implicit. Recipient Fetcheskey from PKG.	Implicit. Recipient Fetcheskey from KDC.
Encryption Key/Target	Recipient key.	Recipient key.	Recipient key.	Recipient key.	KDC public key.

VII. Conclusion And Future Scope

In this paper, the concept of workflow signatures for a secure e-business process is motivated and investigated. This work deals with a centralized approach where not a single task agent is worried about the complexity of the workflow in an inter-organisation. The problem we had in the previous approach that the size of the signature grows linearly with the workflow is not applicable in the proposed work as we are not bothering about the pairings associated with the signature verification. We have also identified some of the unique benefits and also made a study on the comparison of the system. Thus additional benefits can be achieved with this new scheme without any increased assumptions and with no limitations.However, our workflow signature uses some strong trust assumptions even though no additional assumptions are made from the previous one. Constructing a workflow signature scheme with considerably less trust assumptions can make the system more efficient.

References

[1]. R. Buyya, C. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud Computing and Emerging IT Platforms:Vision, Hype, and Reality for Delivering Computing as the Fifth Utility," Future Generation ComputerSystems, vol. 25, pp. 599-616,no. 6, June 2009.

[2]. S.Eckartz, M.Daneva, R. Wieringa, and J.V. Hillegersberg,"Cross-OrganizationalERPManagement: How to Create aSuccessful Business Case?," Proc. ACM Symp. Applied Computing,S. Shin, and S. Ossowski, eds., pp. 1599-1604, Mar. 2009.

[3]. J. Liu, S. Zhang, and J. Hu, "A Case Study of an Inter-EnterpriseWorkflow-Supported Supply Chain Management System," Information& Management, vol. 42, no. 3, pp. 441-454, Mar. 2005.

[4]. P. Grefen, K. Aberer, H. Ludwig, and Y. Hoffner, "CrossFlow: Cross-Organizational Workflow Management for Service Outsourcingin Dynamic Virtual Enterprises," IEEE Data Eng. Bull.,vol. 24, no. 1, pp. 52-57, Mar. 2001.

[5]. G. Alonso, C. Mohan, R. Gunthor, D. Agrawal, A.E. Abbadi, andM. Kamath, "Exotica/FMQM: A Persistent Message-Based Architecturefor Distributed Workflow Management," Proc. IFIP WG8.1Working Conf. Information Systems for Decentralized Organizations,Aug. 1995.

[6]. D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," EUROCRYPT: Proc. Advances in Cryptology, R. Cramer, ed., pp. 440-456, May 2005.

[7]. H.W. Lim and K. Paterson, "Multi-Key Hierarchical Identity-Based Signatures," Proc. 11th IMA Int'l Conf. Cryptography andCoding (IMA '07), S. Galbraith, ed., pp. 384-402, Dec. 2007.

[8]. F. Montagut and R. Molva, "Traceability and Integrity of Execution in Distributed Workflow Management Systems," Proc. 12th European Symp. Research in Computer Security (ESORICS '07), J. Biskupand J. Lopez, eds., pp. 251-266, 2007.

[9]. P. Syverson, D. Goldschlag, and M. Reed, "Anonymous Connections and Onion Routing," Proc. IEEE Symp. Security and Privacy, pp. 44-54, May 1997.

[10]. W. Bagga and R. Molva, "Policy-Based Cryptography andApplications," Proc. Ninth Int'l Conf. Financial Cryptography andData Security (FC '05), A. Patrick and M. Yung, eds., pp. 72-87, Feb.2005.

[11]. V. Atluri, S. Chun, and P. Mazzoleni, "Chinese Wall Security for Decentralized Workflow Management Systems,"J. Computer Security, vol. 12, no. 6, pp. 799-840, Dec. 2004.

[12]. Hoon Wei Lim, Florian Kerschbaum, And HuaxiongWang,"Workflow Signatures For Business Process Compliance," IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 5, September/October 2012.