International Journal of Engineering & Technology, 7 (3.34) (2018) 129-132

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Workflow Signatures for Business Process

Dr.E.Kamalanaban[1], M.Gopinath[2], M.Nandhu[3]

[1] *Professor, Computer Science and Engineering, Vel Tech High Tech Dr Rangarajan Dr Sakunthala Engineering College, Avadi, Chennai- 600062*

[2*]*Assistant Professor, Information Technology, Vel Tech High Tech Dr Rangarajan Dr Sakunthala Engineering College, Avadi, Chennai- 600062. Mail Id: gopitamil23@gmail.com*

[3]*PG Scholar, Master of Computer Applications, Vel Tech High Tech Dr Rangarajan Dr Sakunthala Engineering College, Avadi, Chennai- 600062. Mail Id:nandhum51@gmail.com*

**Corresponding author E-mail: gopitamil23@gmail.com*

Abstract

Workflow signatures are accustomed hold unity of information in which it supports the rational and the order of relationships like AND-join and AND-split, of advancement. Advancement signatures are Digital firm for verifying and proving of business development across some dominant needs. The signing keys are sensible to permit approvals to hold out tasks. Since the signature keys are issued on-the-fly, permission to hold out employment within a work flow will be composed and given energetic at runtime. This paper provides true advancement signature technique, rely on hierarchical unity-placed cryptography, to encounter safety measures by structure workflows. A multi-level validation of data is completed using multi signature binding on each and every message. This can produce an extremely secure and competitive strength to the system. In this paper, an option for the users to generate the key is provided and if the user loses his digital signature, it is providing annotation of recovering the digital signature. Digital signature generated based on identity based signature scheme using hierarchical information which is one of the challenging schemes. Hierarchical information and control flow is controlled by business process automations which is the key focus of this paper.

Keywords: *Cryptography, Digital Signatures, Identity based Signatures, MD5, SPAN*

1. Introduction

In today's business world, forming an alliance with acceptable business partners may be a common strategy for an enterprise to remain competitive by providing a wider vary of product and services to its customers. With an advancement of service-oriented computing, particularly cloud computing, it is additionally applicable for standard corporations to subcontract components of their business processes to a third-party service supplier. This way, the enterprises will think about their core capabilities, while raising the speed and quality of their business processes, and minimizing the business price.

Therefore inter-organizational work flow direction systems, such as enterprise-resource-planning (ERP), supply chain management (SCM) and Cross Flow, play an awfully necessary role in executing business processes with business partners or outsourcers/outsources in a dynamic and timely manner. Briefly, associate inter-organizational work flow management system is employed to model and management the execution of business processes involving a mix of manual and automatic activities between organizations. It may be either centralized or decentralized. The latter is usually most popular for 2 reasons: measurability and autonomous nature of inter-organizational interactions.

During a centralized work flow system, there exists one work flow management engine that is to responsible for distributing tasks to the acceptable execution agents. The central workflow engine also ensures the specified task dependencies by sending tasks to the respective agents only when all requisite conditions are satisfied. In an exceedingly redistributed work flow system, on the opposite hand, a central work flow engine sends the complete work flow to solely the primary execution agent and receives the ultimate output from the last agent within the work flow.

The work flow management during this case is localized, within the sense that every agent within the work flow is accountable not just for corporal punishment associate allotted task. Henceforth, there is a tendency to think about solely redistributed, inter-organizational work flow system. We introduce and investigate the concept of workflow signatures. The scope of this paper is to create a clear hierarchy in validating the data in each business process.

2. Related Work

The users are periodically renewing their non-public keys without interacting with the Public Key generation (PKG). The PKG publically posts the key update data are convenient. However, every user must possess a tamper-resistant hardware device. This assumption makes the answer rather cumbersome. Revocation has been studied within the ID-based setting with mediators [6, 7].

During this setting there is a special semi-trusted third party known as an intermediate World Health Organization holds shares of all users' non-public keys and helps users to rewrite every cipher text. If associate identity is revoked then the intermediate is taught. To prevent serving to the user however should concentrate on a way lot of sensible customary identity based encryption (IBE) setting. In broadcast secret writing, a non-revoked user will facilitate a revoked user gain access to the sensitive data being broad-

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

cast (since this data is that the same for all parties). Association of Business Executives (ABE) is really a generalization of IBE (identity-based secret writing [12]: in associate IBE system, cipher texts are related to only 1 attribute (the identity) [10].
The authority chooses a policy for every user that determines that cipher texts he will rewrite. A threshold policy system would be one during which the authority specifies associate attribute set for the user, and also the user is allowed to rewrite whenever the overlap between this set and also the set related to a specific cipher text is on top of a threshold.
Goyal et al. [14] projected a Key-policy attribute-based encryption (KP-ABE) theme that supports any monotonic access formula consisting of AND, OR, or threshold gates. The KP-ABE format by Ostrovsky, Sahai and Waters [10].
Cloud-based electronic health record (EHR) systems enable medical documents to be exchanged between medical institutions. That is focused on security, performs partial encryption and uses electronic signatures when a patient's document is sent to a document requester. They are used XML encryption and XML digital signature technology, This model works efficiently by sending only the necessary information to the requesters who are authorized to treat the patient in question [15].
Patient's personal information may cause security and privacy problems because it contains sensitive and confidential data about the patient (e.g., health status information, provision of health care, payment for health care, identification of the patient) [13].
This information must be handled with care because its exposure would constitute a severe breach of the privacy of the individual. The EHR system must be designed to guarantee security and privacy when sharing personal patient information [14].
Access control is very important for protecting patient privacy when providing health services. Access control means only transmitting patient documents to authorized doctors. However, most recent access control systems for health services are inflexible due to using role-based access control (RBAC) schemes [15].
Additional security issues may arise due to a lack of consideration for various security factors. Therefore, in order to design a secure and flexible access control system to protect patient privacy in attribute-based access control model using extensible access control markup language (XACML) [16].
The attribute-based access control used in the proposed model can provide flexible and fine-grained access control when compared to existing RBAC schemes. By performing partial encryption of patient privacy-related elements in patient

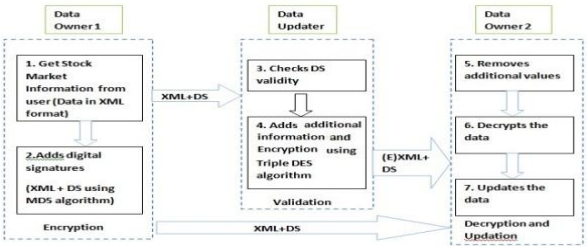


Fig1: Proposed System

Proposed system has three key phases which are Data encryption, Data validation and Data decryption and updation which is depicted in fig.1.Creating a transparent hierarchy in verifying the information in every business method flow is the core extract of this paper. Business rules for a transparent automation method flow must be outlined to identify/segregate the supply and destination points. Additionally, the method involves AND Joins (Process done in parallel to urge the precise outcome), OR Join (Either one in all the method must be done), XOR joins (Finalizing the deciding point).
A Private/Public key will be generated based on a standard identifiers and system parameters. Hierarchical information based on the process flow is decided. This information along with the private/public key will be used to generate a digital signature for signing the message. The length of the key will be differed and it depends on the hierarchy of the process flow in the business flow, based on level of hierarchy the documents via extensible markup language (XML) encryption [17].They used these features for protecting the patient information where as this paper uses the feature for protecting the sharemarketrelatedinformation.
multi key option of signing the message will come into the picture. This paper exactly fits to the task based authorization control, in which task-based cryptographic keys were generated and issued where ever they are required. It assures clarity of positive business traits and managing of special read of business actions. Typically, risk assessment and IT control frameworks are used to support the controls. These controls are then implemented in order to ensure that business processes are compliant with the relevant regulations and laws.

A. Encryption

In this phase, user must have to create his/her own account to login into the system because user credentials are necessary for secured communications. After creating the account the admin needs to validate the user and credentials for accessing the application. SHA1 algorithm is used, which is one of powerful cryptographic hash function which takes an input and produces a 160-bit hash value known as message digest and it is added with the original data for protecting the user details.
SHA1 is more secured compared to AES and DES algorithm, so that this algorithm is used to protect user's details. MD5 is much faster to compute the 128 bit digest for md5 than the 160 bit digest for SHA-1. MD5 is good enough for non-cryptographic purpose; the speed advantage makes it a better choice in most cases.

B. Data Validation

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 sends data to third party (data updater) before sending data to third party, the owner digitally signs the data. That signature is used to verify the data owner and that is helpful for managing some business regularities which is in XML format.

	name	value
1	chevrolet chevelle malibu	130
2	buick skylark 320	165
3	plymouth satellite	150
4	Hyundai	120

Fig2: Original Data

The original data of the user before encryption is shown in fig.2. By using Triple DES algorithm user's original data is encrypted and digital signature is added. After completing the process, the encrypted information is sent to data updater. Below figures fig.3 and fig.4 shows the encrypted data with digital signature in xml format.
Third party is going to verify the encrypted data by using signature in XML. If the signature is invalid, the data will be rejected and the message will be send to data owner. If the XML is valid then the updater is going to amend his values to the owner's data. The Updater sent back data to data owner. Data validation is depicted in fig.3. If the data is not changed by the third party or hackers, the receiver gets the full access to the data on database. In fig.4 the error message while accessing because the data is changed by third party or hackers is shown.



Fig. 3: Valid Information

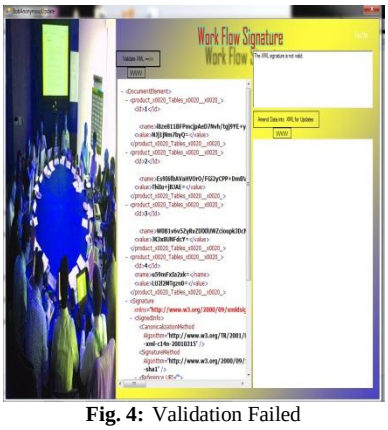


Fig. 4: Validation Failed

C .Decryption and Updation

The Data Owner first, removes additional values sent by updater. Data Owner Decrypt that data. If the data matches with the original Xml data, the xml data is converted to original data format .After the Owner updates the values sent by Updater. Otherwise the data will be taken has invalid.After removing additional values sent by a updater, the information in the xml format look like


```
- <DocumentElement>
- <product_x0020_Tables_x0020__x0020_>
<Id>1</Id>
<name>SEéSGHIJd'ãCEęćHŕIECõEąCśĻhnëčĘ'nģıjćIAijĄčëĻş</name>
<value>ĴÍCœCÍd'rÃëijş</value>
</product_x0020_Tables_x0020__x0020_>
- <product_x0020_Tables_x0020__x0020_>
<Id>2</Id>
<name>ĥdšiRAĄğĬĂIJßÐiõHhćOëgUU'nHd'GJOëã</name>
<value>ĶCéïë'nCGIĕĥş</value>
</product_x0020_Tables_x0020__x0020_>
- <product_x0020_Tables_x0020__x0020_>
<Id>3</Id>
<name>jCEGœERErxëIExHDlDkjxãõśëEõõHãjćd</name>
<value>ĬïõESkIHCãĻş</value>
</product_x0020_Tables_x0020__x0020_>
- <product_x0020_Tables_x0020__x0020_>
<Id>4</Id>
<name>ŕşdHEïãOEćş</name>
<value>ĬķODOjKąEĆCEş</value>
</product_x0020_Tables_x0020__x0020_>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"> <SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference URI="">
<Transforms><Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>Z5KUNFq606K8OXktlZUKVKvHVKs=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>KMQecpKwf5FV4D7NiBxLrUhHcCLn1aTxfbCYucSpBqs
kQ3KqhkfIv8upOxNCgOzMm72Ey8pi1gtPoYTDqsonNU5CJbzl09mvKLn+
S8OLCsTIRgmeq6OynRI76K786WaXSoV+BRB0JpnxPIkE74NQIjWNhxzV
GmTkH4ZUE5Zsh/A=</SignatureValue>
</Signature>
</DocumentElement>
```


After removing additional nodes the information will be decrypted and the decrypted information in the xml format like


```
<DocumentElement>
- <product_x0020_Tables_x0020__x0020_>
<Id>1</Id>
<name>i8ze8BFPmcjpAeD7Nvh/tgj9YE+ykz+CSMMaNbQfowY=</name>
<value>NJj1jNm7byQ=</value>
</product_x0020_Tables_x0020__x0020_>
- <product_x0020_Tables_x0020__x0020_>
<Id>2</Id>
<name>Es9I6fbAVaHVOrO/FGi2yCPP+DmBV2yc</name>
<value>ThiIu+jBJAE=</value>
</product_x0020_Tables_x0020__x0020_>
- <product_x0020_Tables_x0020__x0020_>
<Id>3</Id>
<name>W0B1v6v5ZyRvZDlXlUWZcioupk3DcMis</name>
<value>JK3x8UNFdcY=</value>
</product_x0020_Tables_x0020__x0020_>
- <product_x0020_Tables_x0020__x0020_>
<Id>4</Id>
<name>u59mFxIa2xk=</name>
<value>LU2l2MTgzn0=</value>
</product_x0020_Tables_x0020__x0020_>
- <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
- <SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
- <Reference URI="">
- <Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>Z5KUNFq606K8OXktlZUKVKvHVKs=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>KMQecpKwf5FV4D7NiBxLrUhHcCLn1aTxfbCYucSpBqs
kQ3KqhkfIv8upOxNCgOzMm72Ey8pi1gtPoYTDqsonNU5CJbzl09mvKLn+
S8OLCsTIRgmeq6OynRI76K786WaXSoV+BRB0JpnxPIkE74NQIjWNhxzV
GmTkH4ZUE5Zsh/A=</SignatureValue>
</Signature>
</DocumentElement>
```


Once decryption is completed, the information sent by data owner and data updater will be compared. If both the information are similar means, the information is treated as valid otherwise the information will be taken as invalid. The information is valid means information's are updated otherwise the information's are discarded.

The Owner updates the values sent by Updater. The Original data will be changed based on background verification and different layers of authentication check. After verification the Data Owner gets the updated data.

4. Security Analysis

For analyzing the security performance of the whole proposed system SPAN tool is used which is the simulator of Automated Validation of Internet Security Protocols (AVISPA). AVISPA has four backend tools where as OFMC and ATSE are used for security analysis purpose. Input is obtained in High Level Protocol Specification Language (HLPSL) format or CAS+.

The credentials shared by the key players are validated and it should summarize the report as SAFE which is main objective of the SPAN tool. Security of proposed system is ensured by the summary report of the back end tools OFMC and ATSE derived as SAFE which means it ensures its security and it is shown in Fig.5. As SPAN is the simulator tool for AVISPA, the proposed system is simulated and it is depicted in Fig.6.

% OFMC	**%ATSE TOOL**
% Version of 2006/02/13	SUMMARY
SUMMARY	SAFE
SAFE	DETAILS
DETAILS	
	BOUNDED_NUMBER_OF_SESSIONS
BOUNDED_NUMBER_OF_SESSIONS	TYPED_MODEL
PROTOCOL	PROTOCOL
C:\progra~1\SPAN\testsuite\results\hlpsl GenFile.if	C:\progra~1\SPAN\testsuite\results\hlpsl GenFile.if
GOAL	GOAL
as specified	As Specified
BACKEND	BACKEND
OFMC	CL-AtSe
COMMENTS	STATISTICS
STATISTICS	Analysed : 8 states
parseTime: 0.00s	Reachable : 4 states
searchTime: 0.04s	Translation: 0.00 seconds
visited Nodes: 6 nodes	Computation: 0.00 seconds
depth: 4 plies	

Fig. 5: Results of OFMC and ATSE back end tools

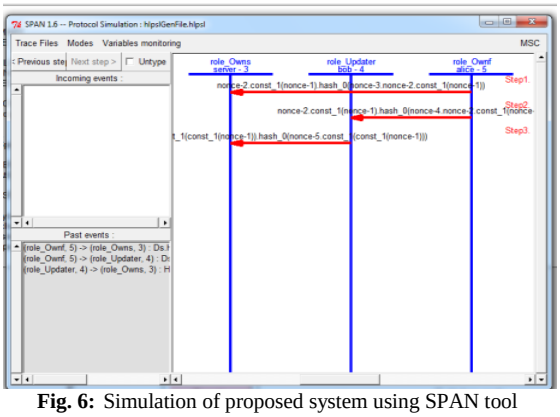


Fig. 6: Simulation of proposed system using SPAN tool

5. Conclusion

The workflow signature takes connections of settings within a workflow, in joining the qualities of a usual sign that is combined to data security and virtue. The workflow signatures can be utilized as evidence that business processes believing on testy administrative workflows are yielding to definite rules. The task depends on cryptographic keys are generate persistent volume sign, and extra effective plan, residue a candid difficulty. This paper provides a secured system for workflow process of business process and evolves security using SPAN tool in which result is obtained as SAFE.

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] M. Naor and K. Nissim. Certi_cate Revocation and Certi_cate Update. In USENIX Security Symposium, 1998.

[3] W. Aiello, S. Lodha, and R. Ostrovsky. Fast Digital Identity Revocation (Extended Abstract). In CRYPTO, pages 137{152, 1998.

[4] D. Naor, M. Naor, and J. Lotspiech. Revocation and Tracing Schemes for Stateless Receivers. In CRYPTO, 2002.

[5] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai. Identity-Based Hierarchical Strongly Key-Insulated Encryption and Its Application. In ASIACRYPT, pages 495{514, 2005.

[6] D. Boneh and M. K. Franklin. Identity-Based Encryption from the Weil Pairing. In CRYPTO, pages 213{229, 2001

[7] B. Libert and J.-J. Quisquater. E_cient revocation and threshold pairing based cryptosystems. In PODC, pages 163{171, 2003.

[8] D. Boneh and M. K. Franklin. Identity-Based Encryption from the Weil Pairing. In CRYPTO, pages 213{229, 2001.

[9] Moni Naor, Benny Pinkas, and Omer Reingold. Distributed Pseudo-random Functions and KDCs. In EUROCRYPT, volume 1592 of LNCS, pages 327–346. Springer, 1999.

[10] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-Based Encryption with Non-Monotonic Access Structures. In Computer and Communications Security, pages 195–203, 2007.

[11] Amit Sahai and Brent Waters. Fuzzy Identity-Based Encryption. In EUROCRYPT, volume 3494 of LNCS, pages 457–473. Springer, 2005.

[12] Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In CRYPTO, pages 47–53.

[13] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, ''Patient controlled encryption: ensuring privacy of and Signature Schemes. In CRYPTO, pages 47–53.

[14] electronic medical records,'' in Proc. ACM Workshop Cloud Comput. Security, 2009, pp. 103–114. [Online]. Available: http://dl.acm.org/citation.cfm?id=1655024

[15] P. Ray and J. Wimalasiri, ''The need for technical solutions for maintaining the privacy of EHR,'' in Proc. 28th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBS), Sep. 2006, pp. 4686–4689. [Online]. Available:http://ieeexplore.ieee.org/abstract/document/4462848/

A. Abbas and S. U. Khan, ''A review on the state-of-the-art privacy preserving approaches in the e-health clouds,'' IEEE J. Biomed. Health In format., vol. 18, no. 4, pp. 1431–1441, Apr. 2014. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6714376/

[16] Extensible Access Control Markup Language (XACML) Version 3.0, OASIS Standard 22, Jan. 2013. [Online]. Available: http://docs.oasisopen.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[17] (Dec. 10, 2002). XML Encryption Syntax and Processing, W3C Recommendation. [Online]. Available: http://www.w3.org/TR/xmlenc-core

[18] Kwangsoo Seol , Young-Gab Kim, Euijong Lee, Young-Duk Seo , & Doo-Kwon Baik.(2018). Privacy-Preserving Attribute-Based Access Control Model for XML-Based Electronic Health Record System, version 6, pages 9114 – 9128.