ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 5, May 2014**

# Digitalised Secure Information Channel Maintanence in Distributed Brokering Systems

E.Prakash, Prof .A.Suresh,

Assistant Professor, Dept of CSE, Asan Memorial College of Engineering and Technology, Chengalpattu, Tamil Nadu, India.

Professor & Head, Dept of CSE, Asan Memorial College of Engineering and Technology. Chengalpattu, Tamil Nadu, India

**ABSTRACT***:* Issues related to sharing information in a distributed system are one of the major practical issues consisting of autonomous an entity which needs to be securely transferred in a heterogeneous multi subdivided systems. Semi-honest nature of the intermediate brokers has been adopted as the base model for adversarial hacking or threats and a secure mechanism to safeguard the system is really wanted information for most of the business owners. Consider a data is navigated from the user to the coordinators via brokers. In that case, there is a lot of possibility for data leakage and the intermediate people can hack the sensitive data of the users. To overcome the possible flaw of information's leakage, the existing system proposes a technique of encrypting the entire data with partial decryption technique to individual intermediate brokers. Unfortunately, security mechanism in validating the end to end users is missed out here and we are trying to incorporate a digital signature based verification system which provides a highest secure data transmission channel.

**KEYWORDS:** Digital Signature, Data Authentication, Data leakage, Privacy.

## I. INTRODUCTION

A company or other organization that engages in the business of trading has several brokers through which the customers or clients can approach the company for shares. There are situation the brokers who act as an intermediate between the organization and the customers can change the quotation in order the gain money for their sake. The preceding limitation can be overcome by the novel based approach with the effective algorithms in order to overcome the problem of communication delimitation between company and customers.

## II.PROPOSED SYSTEM

In existing system many information management applications and other sensitive information which we share with the broker parties and coordinators cannot be stored as a record of secured information. It's the security which is unconditional and does not depend on complicated computational assumptions when the invalid encryption takes place for the brokering control for data overlay. Moreover, the information management system must be robust such that it can still work when some distributed servers are corrupted and hided over the complex analysis.

- They fail to focus on the more wide range of applications for opting security providence.
- The Database with the tuple data does not maintained confidentiality.
- It's not allowing the broker agencies and coordinator parties to look into the unique authenticated information.

ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 5, May 2014**

- The Intermediate broker to easily access and modify the database.

Thus the proposed system allows more complex data to be shared in a secured manner and it also has applications in privacy preserving data. The problem of sharing privately is overwhelmed by our algorithmic approach by providing digital signature of the data, which cannot be identified by other parties extensively. The exertion reported in this paper further explores the modification of other parties between sharing secrets in an anonymous manner, will automatically make the original information to be an invalid one.

- Distributed secure computation system show that our approach seamlessly integrates security enforcement.
- Trust level and accessing privilege providence of unified data access.

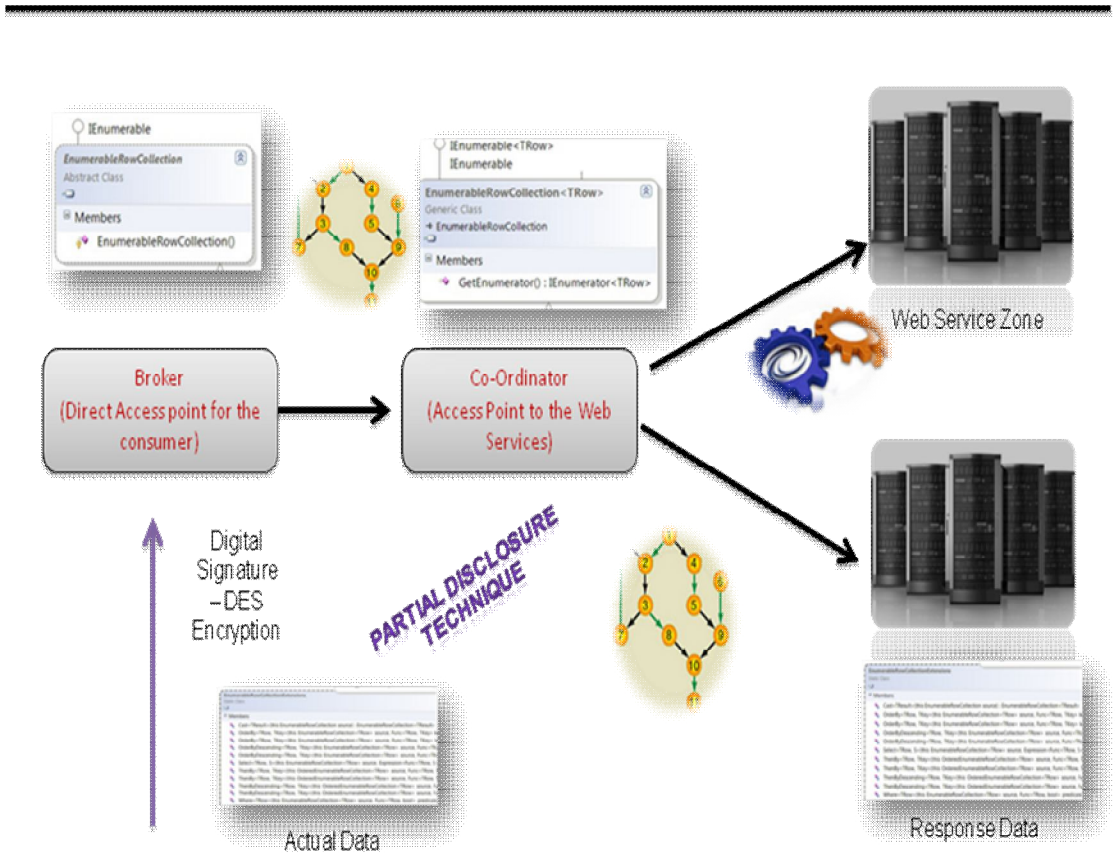


Fig 1 System Architecture

ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 5, May 2014**

## III SYSTEM DESIGN

*A. Data Utilization Module*

Data in the form of request from the client to the organization is utilized. Data ownership refers to both the possession and responsibility for information. The owners have to send the data to the respective receiver using the data distributors. The data distributors who will further distribute the data to the receivers.

*B. Digital Signature zone*

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message. Possibly to ensure that the original content of the message or document that has been sent is unchanged. All role players they should authenticate the data using the procedure of digital signature

*C. XML Signature Verification zone*

XML Signature defines an XML syntax for digital signatures. It uses reference validation and signature validation to validate the digital signature. In this module, the digitally signed documents by the client, intermediates and the organisations are validated in order to check its genuineness.

*D. Partial Disclosure Coordination Zone*

Partial disclosure co-ordination zone is mainly to safeguard the confidentiality between client and organisation thereby preserving the data from the intermediates illegal activities. In this module, the data are partially viewable according to the individual role players who acts as intermediate, this maintain confidentiality and direct dealing between client and organisation.

*E. Web Service Zone*

Web services are XML-based information exchange systems that use the Internet for direct application-to-application interaction. These systems can include programs, objects, messages, or documents. In this module, the data from the client through intermediate persons are placed in a common place. The data's are then accessed by the organisation for providing further request.

## IV RELATED WORK

In [1], Research areas such as information integration, peer-to-peer file sharing systems and publish-subscribe systems provide partial solutions to the problem of large scale data sharing. Information integration approaches focus on providing an integrated view over large numbers of heterogeneous data sources by exploiting the semantic relationship between schemas of different sources. Peer-to-peer systems are designed to share files and datasets (e.g. in collaborative science applications).

In [2], Addressing a conceptually dual problem, XML publish subscribe systems are probably the closely related technology to the proposed research: while PPIB locates relevant data sources for a given query and route the query to these data sources, the pub/sub systems locate relevant consumers for a given document and route the document to these consumers. However, due to this duality, we have different concerns: they focus on efficiently delivering the same piece of information to a large number of consumers, while we are trying to route large volume but small-size queries to much fewer sites. Accordingly, the multicast solution in pub/sub systems does not scale in our environment and we need to develop new mechanisms.

In [3], one idea is to build an XML overlay architecture that supports expressive query processing and security checking atop normal IP network. In particular, specialized data structures are maintained on overlay nodes to route XML queries. a robust mesh has been built to effectively route XML packets by making use of self-describing XML

ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 5, May 2014**

tags and the overlay networks. Kouds et al. also propose a decentralized architecture for ad hoc XPath query routing across a collection of XML databases To share data among a large number of autonomous nodes, studies content-based routing for path queries in peer-to-peer systems. Different from these approaches, PPIB seamlessly integrates query routing with security and privacy protection.

In [4], Research on anonymous communication provides a way to protect information from unauthorized parters. Different protocols have been proposed to allow a message sender dynamically selecting a set of other users and relaying its request. Such approaches can be incorporated into privacy preserving information brokering to protect locations of data requestors and data servers from being known by irrelevant parties in communication. However, aiming at enforcing access control during query routing, PPIB addresses more privacy concerns other than anonymity, and thus faces more challenges.

In [5], finally, many researchers have been proposed on distributed access control. It gives a good overview on access control in collaborative systems. In summary, earlier approaches implement access control mechanisms at the nodes of XML trees and filter out data nodes that users do not have authorizations to access

## V. TECHNIQUES AND ALGORITHM USED

*A. Partial Disclosure Algorithm*

Avoiding disclosure of sensitive info, which includes suppressing all sensitive entries in a table along with a specific number of other entries in the table, which in turn referred as complementary suppression. The idea is to allow each table entry $x_i$ *to be replaced by a convenient* interval

$[x_i - z- i , x_i + z+ i ]$ .

The extreme values of each interval have then to be determined so as to ensure the required protection for the sensitive entries, while minimizing the overall loss of information incurred.

*B. MD5 Algorithm*

MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted *A*, *B*, *C* and *D*. These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed *rounds*; each round is composed of 16 similar operations based on a non-linear function *F*, modular addition, and left rotation.

B. *Digital Signature Algorithm*

Key generation has two phases. The first phase is a choice of *algorithm parameters* which may be shared between different users of the system, while the second phase computes public and private keys for a single user

- Choose $x$ by some random method, where $0 < x < q$.
- Calculate $y = g^x \bmod p$.
- Public key is $(p, q, g, y)$. Private key is $x$..*Signing*

Let $H$ be the hashing function and $m$ the message:

- Generate a random per-message value $k$ where 0<k<q
- Calculate r=($g^k$ mod p) mod q
- In the unlikely case that r=0start again with a different random $k$
- Calculate $s=k^{-1}$ (H(m)+xr)mod q
- In the unlikely case that's s=0, start again with a different random $k$

ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 5, May 2014**

- The signature is (r,s)

*Verifying*

- Reject the signature if (0<r<q) or (0<s<q) is not satisfied.
- Calculate $w=s^{-1} \bmod q$
- Calculate u1=(H(m) w mod q)
- Calculate u2=r.w mod q
- Calculate $r=(g^{u1}g^{u2} \bmod p) \bmod q)$
- The signature is valid if v=r

## VI CONCLUSION

This paper , can use this process for digitalised secure information channel maintainence in distributed brokering systems. In existing information brokering systems suffer from a spectrum of vulnerabilities associated with user privacy, data privacy, and metadata privacy. In this paper, we propose a new approach top reserve privacy in XML information brokering. Through an innovative digital signature scheme, in-network access control, and query segment encryption, digital signature module is used to maintain the privacy of the data from the organization to the customer. In Future validation of digital signature concept has to implement and partial disclosure of data is append to digital signature has send to the customer through the intermediate

## REFERENCES

[1] Boldy Reva.A, Goyal.V and Kumar.V (2012), "Identity-Based Encryption with Efficient Revocation",Proc.ACM Conference and comm.,security,pp.417-426.
[2] Bertino.E, Byun.J.W, Li.T and Sohn.Y.(2009) "privacy Preserving incremental data dissemination" J.Computer Security,Vol 17,no.1,pp.43-68.
[3] Chao Song, Quixia Zhang, Zhan Li (2011), "The Improvement of digital signature algorithm based on elliptic curve cryptography,"Artificial Intelligence Management Science and Electronic Commerce(AIMSEC), pp. 1689–1691.
[4] Chaudhari N.S and Saxena N, (2012) "Secure encryption with digital signature approach for Short Message Service," Information and Communication Technologies pp.803-806.
[5] Chen Hai-peng, Shen xuan-jing, Wei Wei., (2009),"Digital Signature Algorithm Based on Hash Round Function and Self-Certified Public Key System", Education Technology and Computer Science., vol.2, pp.618-624.

## BIOGRAPHY

Mr. E. Prakash., B.E.,M.E.,(Ph.D) works as the Assistant Professor of the Computer Science and Engineering Department in ASAN Memorial College of Engineering & Technology, Chengalpet, Chennai, TamilNadu, India. He has more than 3 years of experience in teaching and his areas of specializations are Network Security and Neural Networks. He has published many of her papers work in national and international conferences.

Dr. A. Suresh., B.E.,M.Tech., Ph.D works as the Professor & Head of the Computer Science and Engineering Department in ASAN Memorial College of Engineering & Technology, Chengalpet, Chennai, TamilNadu, India. He has more than 16 years of experience in teaching and his areas of specializations are Data Mining, Artificial Intelligence, Image Processing, Neural Networks and System Software. He has published many of his research work in national and international journals & conferences and he has published one book in the name of Data structures & Algorithms in DD Publications.