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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Digitalised Secure Information Channel Maintenance in Distributed Broking System

A. Uma Maheswari[1], Mrs.V.Muthamilselvi[2]

PG Student, M.E (CSE), Valliammai Engineering College, Chennai, India[1]

Assoc. Prof/CSE, Valliammai Engineering College, Chennai, India[2]

Abstract: Issues related to sharing information in a distributed system are one of the major practical issues consisting of autonomous entities which need to be securely transferred in subdivided systems. The intermediate brokers have been adopted for adversarial hacking and a secure mechanism to safeguard the system is really required information for most of the organization. The end users are willing to share secure data across the network. Consider a data is navigated from the user to the organization 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. More potential are there for the attacker to deduce some of the most important information's on the whole about the data owner and deduce the data within the data server .To overcome the possible flaw of information's leakage we propose digital signature concept to sign data which is securely transferred. 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, DES encryption, security, privacy, information sharing, brokering system

I. INTRODUCTION

Information sharing is important in recent years which are increasing not only among organizations with common or balancing interests, but also within huge organizations which are becoming more globalized and spread across the network. Along with the sudden increase of information collected by organizations in many realms ranging from business to organization activity, there is an increasing need for interorganizational information sharing to facilitate wide collaboration. While being considered a solution between "sharing nothing" and "sharing everything", peer-to-peer information sharing frame essentially need to create pair wise client-server relationships between each pair of peers, which is not scalable in large scale mutual sharing. Security for organization activity need to distribute information for devising valuable security measures, both within the same organization and across the organization. The activities which are present in the organization cannot arbitrarily open up its database to all other organization activities. Network security provides authentication and confidentiality for sharing information in a network [1].

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. In the context of sensitive data and autonomous data provider, a more realistic and flexible solution is to construct a data-centric overlay consisting of data sources and a set of brokers that make routing decisions based on the content of the data. Such infrastructure builds up semantic-aware index mechanisms to route the data based on their content, which allows user to submit data without knowing data or server location. There are situation the brokers who act as an intermediate between the organization and the customers can change the data in order to gain money for their sake. There are two novel schemes to prevent curious or corrupted coordinators from inferring private information, one is to segment the data brokering automata and the other is to encrypt corresponding data segments so that routing decision making is decoupled into multiple correlated tasks for a set of collaborative coordinators.while providing integrated in-network access control and content-based query routing. 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. Traditionally digital signature concept is used for providing security in network communication. Digital signature widely use hash functions such as

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

MD5 and SHA family. Digital signature is used for signing the data which is sent by user to client, to avoid no hacking process by third parties between user and the client [2].
Information security is mainly focused on these functions must be performed and given below [2]:

A. Authentication:

Each party should authenticate its counterpart.

B. Integrity:

Each party should make sure that the acknowledged messages are not altered or fabricated by other than its counterpart.

C. Confidentiality:

Each party wants to keep the content of its communication secret.

D. Message authentication:

Each party wants to make sure that the received messages do really come from its counterpart.

E. Non-repudiation:

Each party desires to avoid that the counterpart later denies the agreements that it has approved earlier.

II. RELATED WORK

A. Survey of the paper

1) Privacy Preserving Incremental Data Dissemination

In this paper the k-anonymity model and l-diversity model is recently drained for significant attention in the research community. The k-anonymity model mainly focuses on the difficulty of record identification. The l-diversity model built upon the k-anonymity model which addresses the threat of attribute disclosure. These models have yielded a number of precious privacy-protecting techniques. This paper represents "one-time" data dissemination where it does not effectively address today's strong demand for immediate and up-to-date information. It introduces the anonymization techniques for preserving privacy of data dissemination. These include various generalization strategies such as hierarchy-based generalization, single-level generalization, multi-level generalization and hierarchy-free generalization. This project emphasizes a strongest concept of finding anonymous data dissemination. Possible attacks which are present in finding anonymous data dissemination are Record tracing attack, Intersection attack and Difference attack [3]. Disadvantage of this paper are investigation on the inference issues in more dynamic environments where deletions and updates of records are allowed is not discussed in this paper. It does not consider all the inference issues only some of the specific items were considered in this paper [11].

2) Attribute-based encryption

This paper focused on Attribute based encryption determines decryption ability based on a user attributes.In a ABE scheme, multiple attribute-authorities monitor dissimilar sets of attributes and issue corresponding decryption keys to user, and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase technique gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every cipher text, which seems somehow contradictory to the original goal of distributing control over many potentially un trusted authorities[4][8]. A solution has been proposed that removes the trusted inner authority, and protects the users' isolation by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice[4] disadvantage of this paper consist of the system was more complex and the confidentiality depends critically onthe security of the central authority. The methods and techniques used in this project are not efficient and do not contain all the security for the database.

3) XML Information Brokering

Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu proposed to distributed information brokering system satisfies the data with privacy protection using the novel privacy preserving information brokering

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

(PPIB). The automaton segmentation scheme, distributed access control enforcement, and query segment encryption, integrates security enforcement and query forwarding while preserving system-wide privacy. PPIB takes an automation segmentation to provide privacy protection. Automation segmentation is to split susceptible information to largely worthless shares held by multiple parties who collaborate to share the privacy-preserving accountability. PPIB uses automation segmentation to segment the data which was sent by user to server through broker [4][8]. Disadvantage of this paper consist of the IBS suffers from a spectrum of vulnerabilities associated with user privacy, data privacy and metadata privacy.

4) Information Brokering in Distributed Information Sharing

Till now the system provides 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. In this paper, we fail to focus on the most sophisticated and wider range of applications for opting security providence by not allowing the broker agencies and coordinator parties to look into the unique authenticated information. The automation segmentation method, in-network access control, and data segment encryption, PPIB integrates security enforcement and query forwarding while providing comprehensive privacy protection Main problem of this paper, User authentication is not focused [5].

III. PRELIMINARIES

This section reviews the definitions of Information Brokering System, Message Digest Algorithm, Digital Signature and DES encryption.

A.Information Brokering System

Consider an information brokerage system where sensitive information is shared among geographically distributed participants (e.g., users and data sources).architecture of the information system is shown in figure 1.

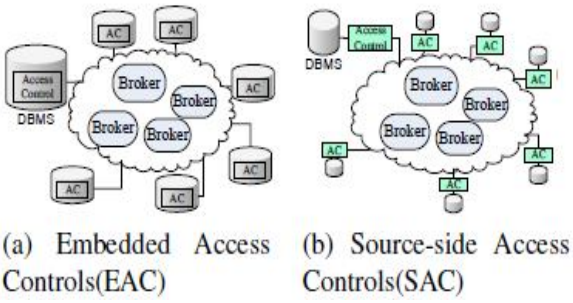

Fig 1: Architecture of Information Brokering System [6]

In general information brokering process, XML queries created by a user are forwarded to data sources by intermediate brokers. Since multiple data source may be relevant to one XML query, replies from all relevant data sources will be merged to provide an aggregate view to the user [9]. In this process, brokers perform as a bridge

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

connecting users and data sources, so they are necessary to know who holds the required data and where they are located. To make the exposition simple, we assume that each broker has a full knowledge of whereabouts of stored data. Therefore, each broker may direct an inquiry to relevant data sources without consulting others [10].

B.Message digest algorithm

An information security consists of lot of encryption and secures algorithms to be used for secure data and verify the integrity of the data. Message Digest is a small piece of data that results encryption. The message digest algorithm consist of message digest algorithm version 5 (MD5) algorithms, secure hash algorithm (SHA) and so on. Message digest algorithm is used for verify the data integrity. MD5 is currently very vulnerable to collision attacks. Consider SHA1 broken since collision attacks are feasible. The MD5 hashing algorithm uses a hash code which is 16 bytes long whereas SHA1 uses a hash code which is 20 bytes long. This means that MD5 executes faster but is less secure than SHA1. From this we can consider that MD5 is not that much secure compared to SHA1 hashing function. In this paper we prefer SHA1 hashing function to verify the data which is to be entered.

C.Digital Signature

Digital signatures are created and verified using Public Key Cryptography that is based on the concept of a key pair generated by a mathematical algorithm, the public and private keys. A digital signature is an encrypted version of a message digest, attached together with a message. Figure 2 shows the digital signature signing and verification process.

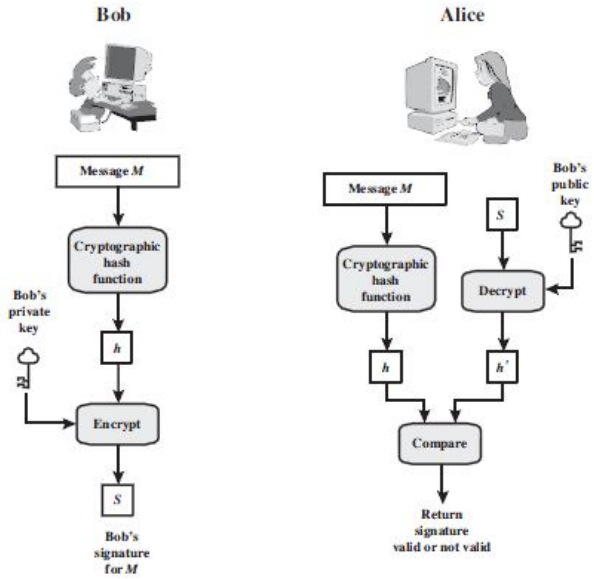

Fig 2: Signing and Verification method [7]

There is no complete trust between the sender and the receiver where authentication is needed. The most striking solution to this problem is the digital signature. The digital signature must have the following properties:

• It must verify the author of the message and at which time and date of the signature.

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

• It must validate the contents at the time of the signature.
• It must be certifiable by third parties, to determine the disputes.

Thus, the digital signature process includes the authentication and confidentiality function from the given data or message.

IV. ENCRYPTION SCHEMES

A.DES encryption

The Data Encryption Standard (DES) is a block cipher that uses secret encryption. Data Encryption Standard is a widely used method of data encryption using a private (secret) key. Symmetric key encryption is also known as single key, secret key, and shared key, private or one-key encryption. In this type of message encryption, both sender and receiver distribute the identical key which is used to both encryption and decryption messages. Sender and receiver just have to indicate the shared key in the beginning and then they can begin to encrypt and decrypt messages between them using that key. In symmetric key there is no secure channel for secret key exchange. Origin and authenticity of message cannot be guaranteed. In asymmetric key encryption, the method of encrypting messages makes use of two keys: a public key and a private key. The public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender. An advantage of public key encryption is detection of tampering where the use of digital signatures in public key encryption allows the receiver to detect if the message was changed in transit. A digitally signed message cannot be customized without invalidating the signature [2].

B.XOR Encryption

The scheme for XOR encryption is unfeasible to invalidate the operation without knowing the initial value of one of the two arguments. For example, if XOR has two variables of unknown values, it cannot tell from the output what the values of those variables are. XOR encryption works on the principle that if you have the encrypted string and the encryption key you can always decrypt suitably. If it does not have the key, it is unworkable to decrypt it without making entirely random keys and attempting each one of them until the decryption program's output is something akin to readable text. [12].

V. PROPOSED SYSTEM

In existing work [5] they focus on information data are send to the web server by using only encryption way but there is no user authentication and there is a possibility of hacking data by third parties between users to client due to some leakages of data, Only encryption and decryption is done while sending the data which is not more secure, these are the main problem of existing system, so they leads to the proposed model. In 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. By using our encryption standard our distributed secure computation system shows that our approach seamlessly integrates security enforcement at the user intensity with a certain trust level and accessing privilege providence of unified data access.

A. Architecture of the proposed work

User send the actual data to the broker which is the intermediate person between the user and the organization, the data is signed with the digital signature.The data is encrypted with xml syntax in broker with the xor encryption algorithm.SHA hashing function is used to sign the message in the signature suite and to verify the data which is entered.

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

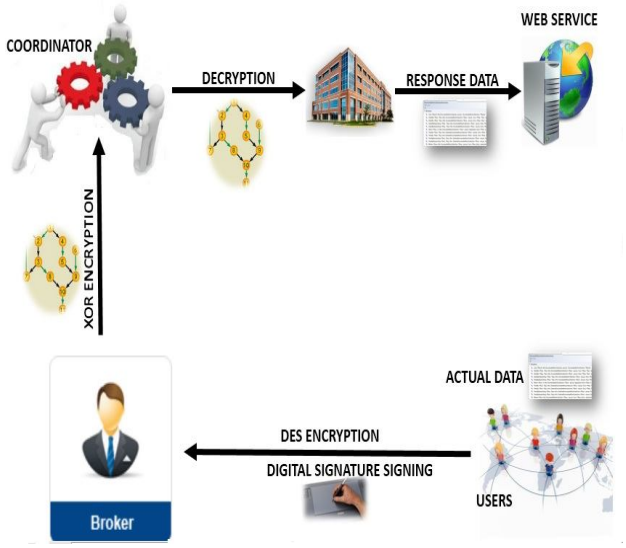

Fig 3: Proposed Architecture

The partial viewable data is transfered to the web service from the client through intermediate person is kept in a common place.Decryption technique takes place to get the actual data from the web service to organization.Response from the organization is sent to client. Proposed architecture shown in figure 3.

B.Process of Digital Signature

User authentication work is not focused on existing work, so third party easily accesses the data. Based on the literature survey, proposed work provide a more security of data by using digital signature concept. Digital signature is an in one direction hash of the original data that has been encrypted with the signer's private key.

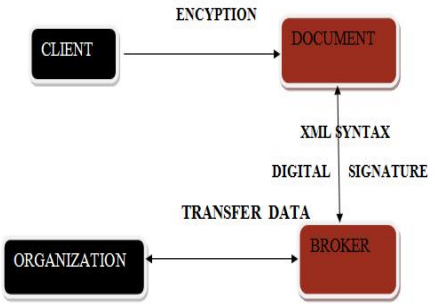

Fig 4: Digital Signature Process

Process of digital signature, all role players such as client, intermediates and the organization should authenticate the data using the procedure of digital signature. Digital signature process shown in figure 4.This digital signature format is the advanced techniques and safe way to transfer the data that is encrypted. By using this data some large quantity of

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

data or detail got encrypted with the use of algorithm. For the verification, the receiving software first uses the signer's public key to decrypt the hash, and then it uses the same hashing algorithm that generated the original hash to generate a new one-way hash of the same data. The software which is received compares the new hash key against the original hash key. If the two hash keys get matched then the data has not changed since the data was signed. The main constraint in the executive of digital documentation is its uniformity, from a legal perspective, affix a signature on a digital document is the fundamental principle on which is based on the main processes of authorization and validation.

C. XML verification process

XML Signature defines XML syntax for digital signatures. It uses reference validation and signature validation to validate the digital signature. In this process, the digitally signed documents by the client, intermediates and the organisations are validated in order to check its genuineness. XML security provides easy-to-use functionality for assigning digital XML signatures to XML documents via XML Signature technology. XML digital signature technology allows you to confirm the authenticity and integrity of XML files, to identity the signing party. The protection of XML Signature provides for XML data is important for transmission of files for everyday business transactions and other official filing documents that are submitted digitally and will likely require the use of digital signatures in the future. XML syntax supports the creation and verification of XML digital signatures. XML file is getting signed using the private key of a digital certificate or a password. The signature can be consequently verified using either the public key that corresponds to the selected certificate or the password specified during the signing process. Checking of the digital signature is main phase in this paper. Verification process is shown in figure 5.

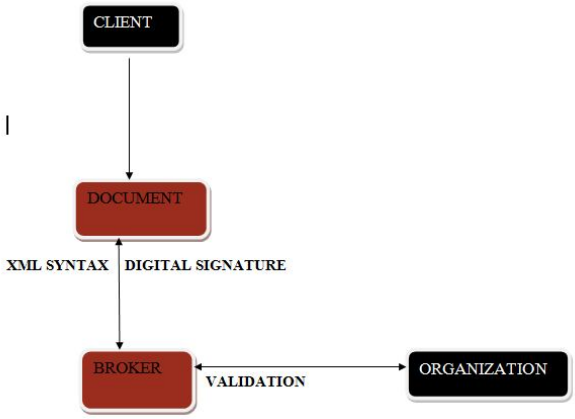

Fig 5: Verification process

C. Benefits of the proposed system

The proposed system is to secure the quotation sent by user for the organization without the intrusion of the broker who is an intermediate person between them, by the using the concept called digital signature. Previously encryption and decryption technique was used for this purpose and it not secure to the core as of our current system which uses digital signature. There is no hacking of data takes place between user and the organization by third parties. If a third party tries to change data for their sake it automatically invalidates the data which is not known by third parties. If the changes applied to data there will be no response from the organization hence secure data is transferred to the organization from user through digital signature.

ALGORITHM:

Digital signature algorithm:

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A. Signing process

For the signing process let us consider a user A which generates a private/public key pair as follows.

1) Create a random integer X_A, such that, $1<X_A<q-1$.
2) Compute $Y_A=\alpha^{X_A} \bmod q$.
3) A's private key is X_A; A's pubic key is {q, α, YA}

To sign a message M, user A first computes the hash m=H (m), such that m is an integer in the range $0\leq m\leq q-1$. A then forms a digital signature as follows.

1) Choose a random integer K such that $1\leq K\leq q-1$ and gcd (K, q-1) =1 .That is, K is relatively prime to q-1 .
2) Compute $S_1=\alpha^K \bmod q$. Note that this is the same as the computation of C_1 for encryption.
3) Compute $K^{-1} \bmod (q-1)$.That is , compute the inverse of K modulo q-1.
4) Compute $S_2=K^{-1}(m-X_AS_1) \bmod (q-1)$.
5) The signature consists of the pair (S_1, S2) [7].

B.Verification process:

Any user B can verify the signature as follows.

1. Compute $V_1=\alpha^K \bmod q$.
2. Compute $V_2= (Y_A)^{S1} (S_1)^{S2 \bmod q}$ [7].

The signature is valid if $V_1=V_2$.

VI. CONCLUSION

The information brokering system that exists suffers from a spectrum of vulnerabilities associated with user privacy, data privacy, and metadata privacy. By compiling the access control policies into the data encryption, accessible client based access control solutions diminish the trust required on the client at the price of a certain extent static way of sharing data. It proposes PPIB, a new approach to preserve privacy in XML information brokering. The quotation quoted by the user is sent through the brokers and corordinatiors to central web service zone where it is manipulated by the organizers. Intermediately to avoid the intrusion, the quotation is secured using the concept of digital signature. Next research includes design an automatic scheme that does dynamic site allotment. Several factors can be considered in the scheme such as the workload at each peer, trust level of each peer, and privacy conflicts between automaton segments. More generally, client-based security solutions deserve a special attention for the new research perspectives they broaden and for their foreseeable impact on a growing scale of applications. And at the last it planned to minimize or eliminate the participation of the administrator node, who decides such issues as automaton segmentation granularity.

REFERENCES

[1].Rakesh Agrawal Alexandre Evfimievski _ Ramakrishnan Srikant, Information Sharing across Private Databases.
[2].http:\\Wikipedia.com.
[3].Ji-Won Byun, Tiancheng Li, Elisa Bertino, Ninghui Li, Privacy-Preserving Incremental Data Dissemination.
[4]. Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu Automaton Segmentation: A New Approach to Preserve Privacy in XML Information Brokering, 2007.
[5].Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu,Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing, IEEE 2013.
[6].Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, Prasenjit Mitra, Wang-Chien Lee, and Chao-Hsien Chu, In-broker Access Control for Information Brokerage Systems.
[7].Cryptography-network-security-5th-edition William stalling Copyright © 2011, 2006 Pearson Education, Inc., publishing as Prentice Hall.
[8]. F. Li, B. Luo, P. Liu, D. Lee, P. Mitra,W. Lee, and C. Chu, "In-broker access control: Towards efficient end-to-end performance of information brokerage systems," in Proc. IEEE SUTC, Taichung, Taiwan, 2006, pp. 252–259.
[9]. I. Manolescu, D. Florescu, and D. Kossmann, "Answering XML queries on heterogeneous data sources," in Proc. VLDB, 2001, pp. 241–250.
[10]. S. Rizvi, A. Mendelzon, S. Sudarshan, and P. Roy, "Extending query rewriting techniques for fine-grained access control," in Proc. SIGMOD'04, Paris, France, 2004, pp. 551–562.
[11]. Seyed Hossein Ahmadinejad_ Mohd Anwar† Philip W. L. Fong_ Inference Attacks by Third-Party Extensions to Social Network Systems.
[12]. E. Anupriya*, Amit Agnihotri, Encryption using XOR based Extended Key for Information Security – A Novel Approach, / International Journal on Computer Science and Engineering (IJCSE).