ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

HECC-CHAP BASED PRIVACY PRESERVATION IN DISTRIBUTED INFORMATION SHARING

Mr. Jay Prakash Maurya*, Mr. Surendra Nagar, Swati Upadhyay
* Dept. of computer Science IES College of Technology Bhopal, India,
Dept. of Computer Science IES Institute of Tech. & Mgmt. Bhopal, India
Dept. of computer Science IES College of Technology Bhopal, India

ABSTRACT

Dept. of computer Science Security is an important issue during the transmission of data. Privacy Preservation enables various users to send their data to the server privately so that the external users can't access the data. Distributed Information Sharing also enables the facility of privacy preservation. Since various technique are implemented for providing privacy in distributed information sharing. Here in this paper a new and efficient technique is implemented for providing privacy preservation in distributed systems as well it also reduces communication time and cost.

KEYWORDS: Distributed Systems, PPIB, IBS, HECC, CHAP, Challenge Value, Inference Attack.

INTRODUCTION

Due to enormous quantity of susceptible data or information are transmitted over open networks and stored in web-easy to get to databases, and consequently privacy of these data has turn out to be a peak precedence over another thing. Decades of follow a line of investigation in cryptography and security have consequences in an well-designed presumption that give you an idea about in standard, how to achieve approximately any computational task in a privacy-preserving manner, but there is a wide gap between theory and put into practice: Currently, most people and organizations have no easy way to protect the confidentiality of their sensitive data in sensible networked in open environments.

When users access a service in the Internet e.g., an online shopping site, payment to a news feed, remarking an entry in a blog, etc., the confirmation techniques and user's data management is entrusted to the distinctiveness contributor. Thus, the uniqueness provider put offs the users from indication up and transfer their private information openly to the services they want to use. The service only gets the information sent by the identity provider, which may hide the real identity of the users, hence preserving their privacy. In the susceptible data and autonomous data holders, a more sensible and adjustable explanation is to put up a data centric spread over the surface [1], [2].

Privacy concerns arise in inter organizational information brokering since one can no longer assume brokers controlled by other organizations are fully trustable. The entities are willing to share information across their databases. Nevertheless, no entity is willing to disclose its private data to other entities due to privacy concern. Typical applications of privacy preserving information sharing problem include document sharing, shared medical databases, etc [9]. Various solutions have been proposed to preserve privacy in distributed information sharing systems. As the major source that may cause privacy leak is the metadata i.e., indexing and access control, secure index based search methods may be accepted to contract out metadata in encrypted form to entrusted brokers. Information brokering systems work on two extremes of the spectrum; either the query-answering model to establish pair-wise client-server connections for on-demand information right of entry, where examines are fully self-sufficient but there be deficient in arrangement extensive synchronization, or the distributed database model, where all examines with modest self-sufficiency are supervised by a incorporated DBMS.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

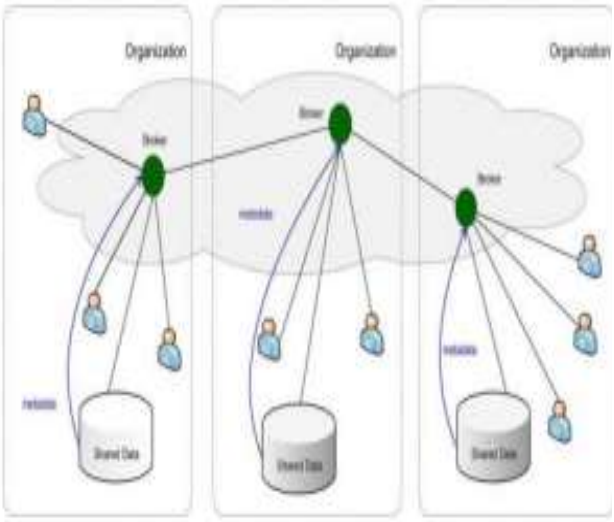

Fig 1– Overview of the IBS infrastructure [5]

Databases of different organizations are connected through a set of brokers, and metadata e.g., data summary, server positions are move forwarded to the local brokers, which supplementary announce some of the metadata to additional brokers. Queries are sent to the local broker and routed according to the metadata in anticipation of accomplishing the correctly data server's. In this approach, a large number of information foundations in different organizations are insecurely join together to provide a unified, transparent, and on-demand data right to use. Brokers are assumed to enforce security check and make routing decision without knowing the content of both query and metadata rules. This problem deals with a setting where a set of parties with private inputs wish to jointly compute some function of their inputs. It may include the data sources and a set of brokers helping to locate data sources for queries [3], [4]. Mechanisms to route the queries based on their comfortable, which permits users to submit queries not including be acquainted within data or server location. At the same time as privacy preserving full control over the data and wide-ranging confidentiality of their users. A number of information systems have been expanded to provide well-organized and protected information distribution [5]. The problem of balancing peer autonomy and system coalition is still challenging.

LITERATURE SURVEY

A Distributed Information Brokering System (DIBS) is a peer-to-peer overlay network that comprises diverse data servers and brokering components helping client queries locate the data server [6]. Federated information system with diverse participants (from different organizations) such as data manufacturers, data users, or both necessitate of cross organizational information sharing naturally happens. On the other hand, different types of applications often require different forms of information distribution. Even though the Internet and a variety of virtual private networks provide good data communication links, there are major challenges in following:

- Achieving scalable, agile and secure remote access of distributed data;
- Handling the heterogeneity among data management organizations and data formats which are not until the end of time arrangement and may be unable to get along with each other;
- Handling the dynamics of modern business applications where new scheme constituents may become known everyday; and
- Location discovery: To begin these confronts, mediation and federation based information brokering technologies have been proposed.

In particular, recent extensible Markup Language (XML) has become a promising solution by integrating incompatible data while protecting semantics. An XML based information brokerage arrangement encompass data sources and brokers in the same way, hold XML documents and document distribution Information [7]. In such systems, databases can be queried through brokers with no schema-relevant or geographical difference being noticed.

In recent trends, organizations raise an increasing need of information sharing to facilitate extensive collaboration among business to government agencies. In olden days Information brokering system (IBS) which acts as intermediate brokers which make decision routing between the query requester and data server by trusting third party. To overcome the trusted third party IBS, extended into privacy preserving for exchanging multiple stakeholders information.

Attribute Correlation Attack using predicates which are used to find a specific node or a node that contains a specific value in XML query which describes conditions that carry sensitive and private data for an e.g., name, SSN, credit card number, etc. [5]. If an attacker captures a query with multiple predicates or combination predicate appearances, the attacker can show a relationship the attributes in the predicates to understand perceptive information concerning data owner. Inference attack, A procedure which combines known facts to produce "infer" new facts, which makes use of premises, such a severe privacy leak

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

occurs when an attacker obtains more than one type of sensitive information and learns explicit or implicit knowledge about the stakeholders through association.[5] By implicit, we mean the attacker infers the fact by estimating. For example, an attacker can guess the distinctiveness of a demand or from her query position e.g., IP address meanwhile, the identity of the data owner could be explicitly learned from query content e.g., name or SSN.

Access control is an integral part of databases and information systems [8]. Granularity of access control refers to the size of individual data items which can be authorized to users. Current day database applications, with large numbers of clients, have need of fine-grained right of entry manage methods, at the level of individual tuples, to control which parts of the data each user can access. Fine-grained access control is often enforced in the application code, which has numerous drawbacks; these can be avoided by specifying/enforcing access control at the database level. A novel fine-grained access control model based on authorization views allows authorization transparent querying; that is user queries can be expression in conditions of the database relatives, and are convincing if they can be answered using only the information contained in these authorization views. Query validity can be checked by a set of powerful set of inference rules. We demonstrate the practicality of our techniques by describing how an existing query optimizer can be extended to perform access control checks by incorporating these inference rules.

An XML brokerage system is a distributed XML database system that comprises data resources and brokers, which in that order grasp XML documents and document distribution information [4]. However, all existing information brokerage systems view or handle query brokering and access control as two orthogonal issues: query brokering is a system issue that concerns costs and concert, while right of entry be in charge of is a security matter that anxieties information secrecy. Consequently, right of entry manage exploitation approaches in terms of where and when to do right of entry manage and the contact of such approaches on end-to-end system concert are forget by continue livening information brokerage systems. As well, data source side right of entry control organized way is taken for contribution as the right thing to do. We confront this conventional, taken-for-granted right of entry organize organized method, and dispute that query brokering and access control are not two orthogonal issues because access control deployment strategies can have a significant impact on the whole systems end-to-end performance. Here author has proposed the first in-broker access control deployment strategy where access control is pushed from the boundary into the sensitivity of the information brokerage system.

PROPOSED METHODOLOGY

The proposed methodology implemented here is based on the combinatorial method of applying challenge handshake authentication protocol and Hyper Elliptic Curve Cryptography.

CHAP Protocol

Step 1: User send a request to system for challenge value.
Step 2: System take challenge value.
Step 3: System calculate timestamp T_1.
Step 4: System take password value.
Step 5: System send challenge value + T1.
Step 6: User received challenge value + T1.
Step 7: User calculate current timestamp T2.
Step 8: User calculates total transmission time = 2 * (T2 - T1) + processing time.
Step 9: User adds transmission time + t1 to tot_time.
Step 10: User take password.
Step 11: Users determine MD5 hashing function on challenge value + pwd + tot_time.
Step 12: User calculate MD5 hashing on this data.
Step 13: User send this data to system.
Step 14: system received data D1.
Step 15: system calculate timestamp T3.
Step 16 System determines (challenge value + password + T3).
Step 17: System determines MD5 hashing on (challenge value + password + T3).
Step 18: If it matches then session is valid. Cheek whether the password valid or not if valid send allowed else send not allowedelse session expires.
Step 19: User will show whether session expires or not.

If not expired then whether password valid or not.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

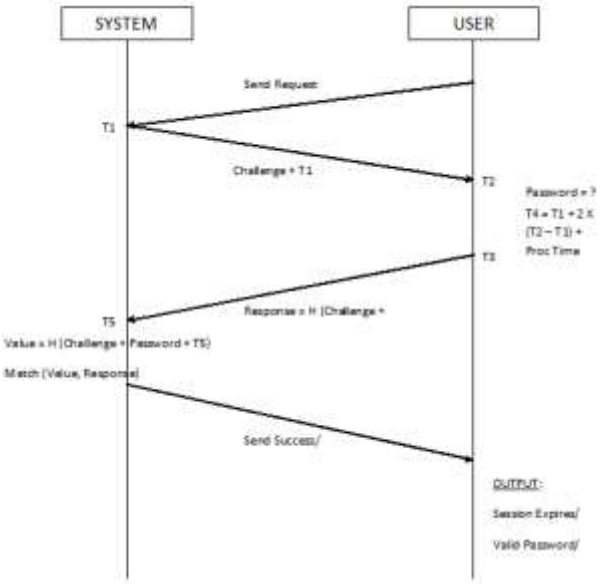

Figure 2. Architecture of CHAP Protocol

HECC

A hyper elliptic curve C of genus g defined over a field Fq of characteristic p is given by an equation of the form

$$y^2 + h(x)y = f(x)$$

Where h(x) and f(x) are polynomials with coefficients in Fq with deg h(x) <=g and deg f(x) =2g+1. An additional requirement is that C is not a singular curve. If h(x) =0 and p>2 this amount to the requirement that f(x) is a square free polynomial. In general, the condition is that there are no x and y in the algebraic closure of Fq that satisfy the equation 1.

Hyperelliptic curve cryptosystems were first suggested for cryptographic use in 1988 and it took almost 10 years until they were implemented. The first two contributions listed implemented Cantor's algorithm with polynomial arithmetic, whereas the others used explicit formulae. Aware of several practical advantages, the research community recently implemented HECC on embedded processors using characteristic two fields. We only present a brief introduction to the theory of hyperelliptic curves.

Let F be a finite field and $\bar{F}$ be the algebraic closure of F. A hyperelliptic curve C of genus g≥1 over the field F is defined as the following equation:

$$C: y^2 + h(x)y = f(x)$$

The solutions (x,y) are points which satisfy the

equation C and the partial derivative equations 2y +h(x) = 0 and h'(x)y –f'(x) =0

RESULT ANALYSIS

The figure shown below is the analysis and comparison of Computational time on the basis of keywords required for the encryption during the information sharing.

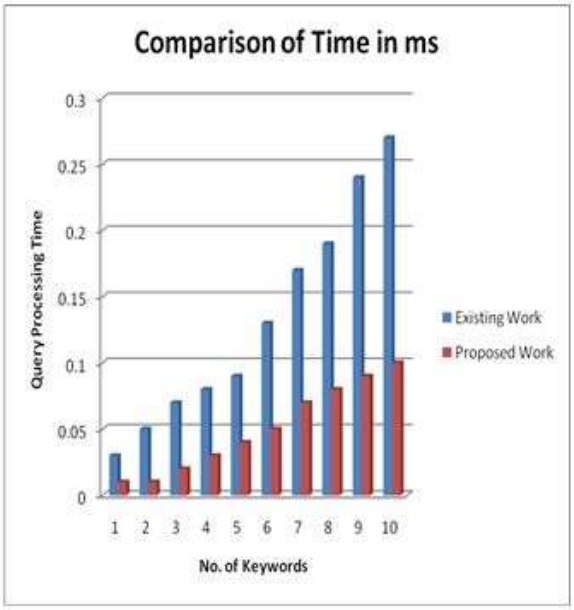

Figure 3. Comparison of Computational Time

The figure shown below is the analysis and comparison of average encryption taken for a number of keywods. The proposed methodology shows less average encryption time as compared to the existing technique.

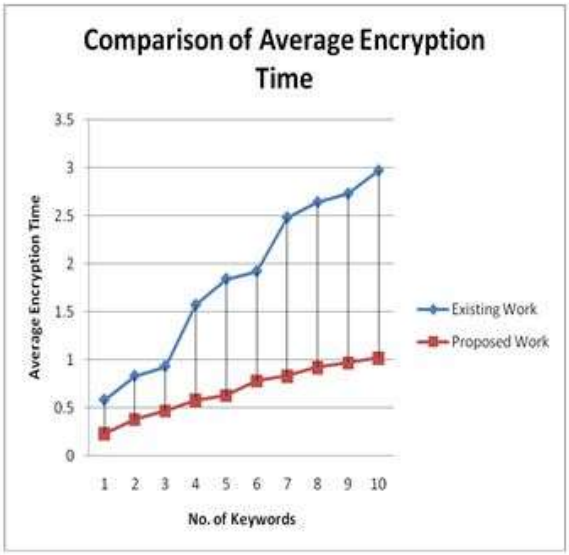

Figure 4. Comparisonn of Average Encryption Time

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

The figure shown below is the comparison of communication cost of the existing and the proposed work. The proposed methodology implemented here provides less communication cost as compared to the existitn technqiue.

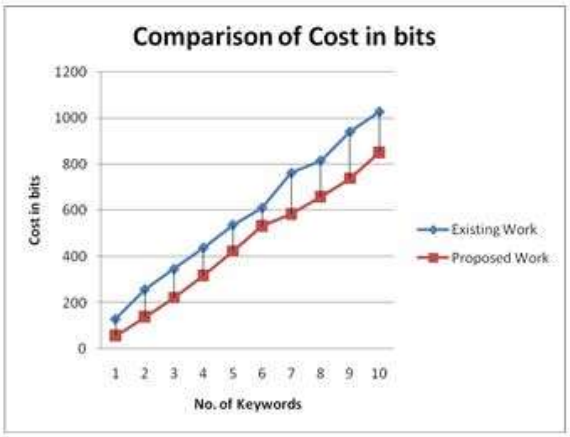

Figure 5. Comparison of Communication cost

The figure shown below is the analysis and comparison of Total number of Keys generated on the basis of keywords required for the encryption during the information sharing.

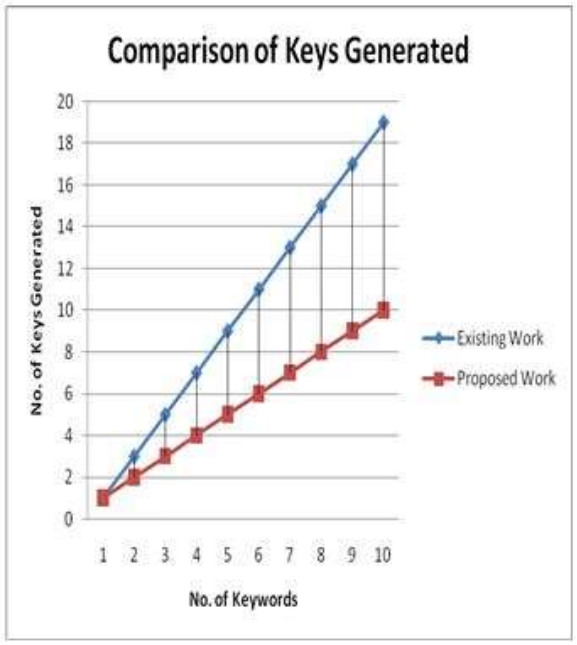

Figure 6. Comparison of No. of Keys Generated

The table shown below is the analysis of various types of atttacks prevented by the exitsing and the proposed methdoology.

Attacks	Existing Work	Proposed Work
Replay Attack	No	Yes
Identity Disclosure Attack	No	Yes
Public Verifiability	Yes	Yes
Confidentiability	No	Yes
Eavesdropping	Yes	Yes
Additional Secuity	No	Yes

Table 1. Analysis of different attacks Prevention

CONCLUSION

The proposed methodology implemented here for providing privacy preservation during the sharing of data especially in distributed information systems. The existing technique implemented for the privacy preservation enables distributed information sharing and prevents attribute co-relation attacks and inference attack. But the technique implemented doesn't provide a load balancing. The proposed methodology implemented here provides security from various attacks as well as it requires less communication time and takes less encryption time as compared to the existing technique. The methodology also provides low communication cost.

REFERENCES

1. X. Zhang, J. Liu, B. Li, and T.-S. P. Yum, "CoolStreaming/DONet: A data-driven overlay network for efficient live media streaming," in Proceedings of IEEE INFOCOM, 2005.
2. A. C. Snoeren, K. Conley, and D. K. Gifford, "Mesh-based content routing using XML," in SOSP, pp. 160–173, 2001.
3. M. Franklin, A. Halevy, and D. Maier, "From databases to dataspaces: a new abstraction for information management," SIGMOD Rec., vol. 34, no. 4, pp. 27–33, 2005.
4. 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, 2006 pp. 252–259.
5. F. Li, B. Luo, P. Liu, D. Lee and C.-H. Chu," Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing," IEEE Transaction 2013.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

6. E. Damiani, S. di Vimercati, S. Paraboschi, and P. Samarati, "Securing {XML} documents," in Proc. EDBT 2000, 2000, pp. 121–135.
7. A. Carzaniga, M. J.Rutherford, and A. L.Wolf, "Arouting scheme forcontent-based networking," in Proc. INFOCOM, Hong Kong, 2004,pp. 918–928.
8. 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.
9. R. Agrawal, A. Evfimievski, and R. Srikant. Information sharing across private databases. In Proceedings of the 22nd ACM SIGMOD international conference on Management of data, pages 86–97, 2003.