International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 12, December-2014

An Efficient Hybrid Technique for Information Sharing using HECC and CHAP

Swati Upadhyay
Dept. of Computer Science
IES College of Technology
Bhopal, India

Prof. J P Maurya
Dept. of Computer Science
IES College of Technology
Bhopal, India

***Abstract*— Privacy Preserving is used to preserve sensitive information in the network. Security is the quality of being secure from any harm. Nowadays, sharing the information between organizations becomes common to increase the extensive collaboration. Information Brokering will make routing decisions to direct client queries to the requested data servers. Securing the persons private data through brokers is less in the information brokering system. Here in this paper a new concept for providing security using Challenge Handshake Authentication Protocol and Identity based HECC is implemented.**

***Index Terms*— Information Sharing, Privacy Preserving, Distributed System, IBS, HECC, ECC.**

I. INTRODUCTION

With the growing internet technology it may require to establishing rules to regulate the privacy of inhabitants in the treatment of sensitive personal data such as medical financial records and much big organizational data. Such rules must be admiration by software used in these areas. The regulatory statements are somewhat informal and must be understand with awareness in the software interface to private data. An additional issue of increasing interest in starting and proving those enterprises, their products workflows, and services are in compliance with relevant privacy legislation. We concentrate on problems related to sharing information in a distributed system consisting of autonomous entities, each of which embraces a private database.

ECC are a generalization of elliptic curve cryptosystems (ECC) and were recommended for cryptographic applications in 1988 by Koblitz. Use of hyperelliptic curve cryptosystems (HECC) by narrowing the performance gap between elliptic curve (EC) and hyperelliptic curve cryptosystems. We were able to reduce the complexity of the group operation for small genus hyperelliptic curves and we provide efficient algorithms for the computation of the hyperelliptic curve cryptosystem. Hyperelliptic curve cryptography is the fast public key cryptographic technique with high efficiency and security [1], [2]. In 1988, Neal Koblitz suggested a new higher genus curve for cryptographic purpose known as Hyperelliptic Curve Cryptosystem. HECC has more advantage such as shorter key size, less computational overhead, high security, require less memory space and consume less power.

The authentication method depends upon a secret shared between the authenticating party (authenticator) and the party being authenticated (requestor). CHAP is a three-way handshake authenticating the requestor only. CHAP is a challenge-response protocol. The challenge sent by the authenticator to the requestor must be unpredictable (e.g., pseudorandom) and globally and temporally unique; otherwise, replay attacks would be possible. The 32-bit CHAP challenge can be determined in a similar way to the "magic number" chosen during the LCP negotiation [3].

II. THEORETICAL BACKGROUND

A strongly communicated and more modern research area is privacy preserving data mining and sharing across distributed data sources [4], [5]. While the data-as-a-service circumstances talk about exceeding reveal the increasing needs for integrating and querying data across distributed and self-sufficient data sources, it stay behinds a confront to make certain assurance to provide privacy, interoperability, and scalability for such data services. It follows the secure multi-party computation model and the main objective is to ensure that data is not making known among participating parties while allocating assured mining or querying task to be carried out. Specialized protocols are proposed for various mining tasks with changeable degree of accuracy, security and cost.

Doing so allocates us to provide a structure that explains the difficulty of managing privacy constraints in web personalization in a common fashion, to take advantage of commonalities among unusual requires for privacy, personalization, to dynamically update different privacy and personalization strategies in a modular fashion, not requiring that the user modeling server be completely rebuilt upon each transform. If privacy considerations are in use into account in the design of computer systems, they restrain the probable design space for such arrangements. Solutions that breach privacy constraints cannot be think any more.

Privacy constraints for computer systems stem first and foremost from two sources, namely from privacy laws and regulations and from personal privacy expectations of the computer users. Figure 1 shows the hierarchy of these constraints with a focus on privacy laws and regulations [6].

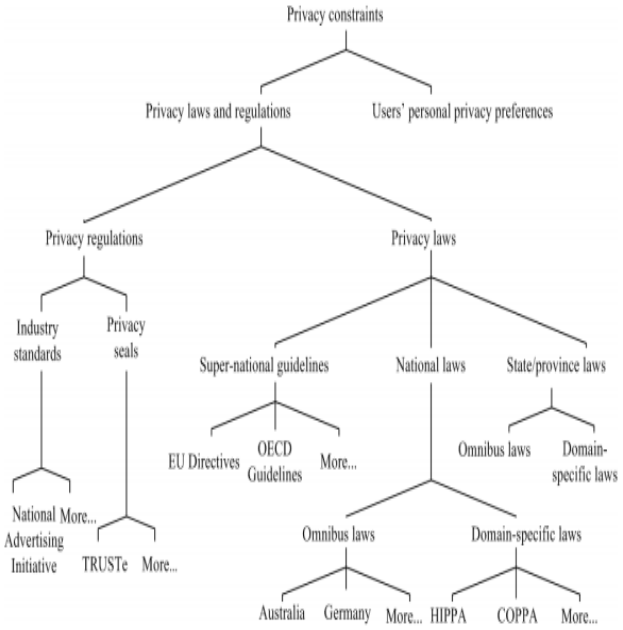

Figure 1: The Hierarchy of Potential Privacy Constraints [6]

III. Literature Survey

In this paper [7], author has proposed a new method to preserve privacy of multiple stakeholders involved in the information brokering procedure to preserve privacy in XML information brokering. Here they firstly define two privacy attacks, i.e. inference attack and attribute-correlation attack, and also they suggest two countermeasure plans automaton segmentation, query segment encryption and in-network access control to securely share the routing decision-making responsibility among a selected set of brokering servers. With small consideration drawn on privacy of user, data, and metadata during the design stage, existing information brokering systems suffer from a spectrum of vulnerabilities associated with user privacy, data privacy, and metadata privacy. Here author [7] has suggested that it is very resistant to privacy attacks using End-to-end query processing concert and system scalability are also estimated and the effects show that there method is efficient and scalable.

First, at present, site distribution and load balancing in PPIB are accomplished in an ad-hoc manner. Then next step of examine is to design an automatic method that does dynamic site distribution. A number of factors can be thinker about in the method such as the workload at each peer; trust level of each peer, and privacy conflicts between automaton segments but these factors is a challenging. Second, they get would like to enumerate the level of privacy protection achieved by PPIB. Finally, they plan to reduce or neglect the participation of the administrator node, who decides such issues as automaton segmentation granularity. A main goal [7] is to make PPIB self-reconfigurable. With widespread security analysis and experimental results; they show that their approach effortlessly incorporates security put into effect with query routing to provide system-wide security with not important operating cost.

In this paper [8], author has presented a privacy preserving repository for integrating data from various data sharing services without central authorities is presented. Using their repository, only bring together the minimum amount of information from data sharing services based on user's addition requests, and data sharing services can control our repository to use their shared information only for user's integration requests, but not other reasons can update, control the access and limit the usage of their shared data instead of submitting data to authorities, and consequently, their repository will encourage data sharing and integration. Here author compare between their own repository and existing central authorities but the major differences are: 1) their repository collects data from data sharing services based on user's integration constraints to a certain extent than all the data from the data sharing services as continue living central authorities. 2) While be presenting central authorities have complete rule of the collected data, the competence of our repository is controlled to computing the integration consequences necessitated by users and cannot get other information about the data or use it for other intentions. 3) The data collected by our repository cannot be used to generate other consequences except that of the particular data integration request, and for this reason the cooperation of our repository can only make known the results of the specified data integration request, while the negotiation of central authorities will make known all data.

In this paper [9] author examined the consequence of enlarging the subsisting up to date in privacy preserving data mining to grid partitioned data, i.e. data which is horizontally as well as vertically partitioned. Privacy preserving decision tree initiation via ID3 in the storage place everywhere the training data is horizontally or vertically distributed data. Additionally, they think about the equivalent problem in the storage place where the data is both horizontally and vertically distributed, circumstances here they reduce in importance to as grid partitioned data. Here they presented an algorithm for privacy preserving ID3 over horizontally partitioned data involving more than two parties. For grid partitioned data they talk about two different estimation techniques for preserving privacy ID3, specifically first integration horizontally and just beginning vertically or first merging vertically and next expanding horizontally. Here author has suggested the first to formalize the concept of grid partitioned data. And then next to establish privacy preserving data mining over grid-partitioned data. Here author give you an idea about by means of a complexity analysis that the earlier estimate technique is the more proficient. This idea gives you an idea about that this situation is of enormous significance to real world circumstances and various applications. Then they maintained by formally defining horizontally, vertically and grid partitioned data.

In this paper [10], we proposed a new classifier using two-layer architecture that enables SMC techniques that it is feasible to build a privacy preserving decision tree classifier with SMC techniques by hiding the identity of the parties taking part in the classification process using UTP. These

computations could occur between mutually un-trusted parties or even between participants. Nowadays, to accomplish such calculations one entity must more often than not know the inputs from all the contestants on the other hand if nobody can be trusted an adequate amount of to know all the inputs so the privacy will become a most important apprehension. Additionally they may possibly illustrate that intermediate result is determined by every party independently and send only intermediate result to Un-trusted Third Party (UTP) not the input data. All the way through the communication between Un-trusted Third Party (UTP) and all party final result is carried out and also necessitates less memory space and also provides fast and easy computations. Using this protocol [10], classification will approximately secure and privacy of individual will be preserved. Additional growth of the protocol is anticipated in the intelligence that for joining multi-party attributes using a trusted third party can be used. Here they are progressing work in this field to extend new classifier for building privacy preserving decision tree classifier using grid partitioned data and to investigation new in addition to existing classifiers. Here the author [10] has to study how to build privacy preserving two-layer decision tree classifier, where database is horizontally partitioned and exchange a few words their transitional consequences to the UTP not their private data. Using this protocol, an UTP allows well-designed solutions that meet privacy constraints and accomplish adequate performance.

In this paper [11], author has analyzed privacy issues in content-based publish/subscribe networks the problem of end-user privacy in content-based publish/subscribe (CBPS) networks. Consecutively to solve this problem with cryptographic tools here they analyzed the link between privacy and confidentiality and identified two necessary confidentiality constraints, specifically publisher and information confidentiality. This led us to the more wide-ranging problem of routing encrypted occurrences using encrypted subscription filters. This problem of secure routing requires two main primitives, that is to say structure of encrypted routing tables with aggregation of encrypted filters and secure look-up of encrypted events with encrypted routing tables to distribute the occurrences proficiently. These two primitives have to be designed collectively with the other classical primitives with the intention of solve the privacy-preserving routing which had no accessible explanation.

Then author [11] presented a solution to this problem based on multiple layer commutative encryptions, the first solution that avoids key sharing among end-users and targets an enhanced CBPS model where brokers can also be subscribers at the same time. MLCE allows brokers to perform secure transformations without having access to the data that is being shifted. Brokers can certainly remove or add an encryption layer without destroying the others and consequently perform aggregation, routing tables building or look-up on private data protected by the some other layers. Privacy is thus definite among all nodes, together with subscribers and eavesdropping outsiders. One possible solution [11] suggested by author has uses the Pohlig-Hellman cryptosystem, and is the first scheme which enables privacy preserving routing with no shared secret between end-users. Hence, key management is straightforward and restricted. Another key characteristic of this protocol is that it allows brokers to be subscribers at the same time although preserving privacy of all nodes which is demanding for peer-to-peer applications. This protocol can also be modified to endure collusion attacks at a confident performance cost. As expectations effort, author has been determined to develop these methods by improving their elasticity concerning the network topology and the contribution filter format. Here they would like certainly to expand subscription filters include logical expressions.

In this paper [12] author provide a organized investigation of the reasons of this problem; and finish that accessible secure information sharing technologies trust models, which are based on certified attributes and it cannot sustain efficient information sharing among government agencies, which have need of an interest-based trust model and protocols cannot make available an adequate amount of incentives for government agencies to share information with each other without perturbing that their own interests can be put in danger and to solve this information sharing problem. Although trust-based information access is well considered in existing trust models, which are based on certified attributes, cannot support effective information sharing among government agencies, which requires an interest-based trust model. To solve this information sharing problem, author suggested [12] an innovative interest-based trust model and a new information sharing protocol, where a people of information sharing policies are combined, and information exchange and trust cooperation are interleaved with and mutually dependent upon each other. As well, an accomplishment of this protocol is accessible using the emerging technology of XML Web Services. The implementation is entirely well-suited with the Federal Enterprise Architecture reference models and can be openly integrated into existing E-Government systems.

Besides, an implementation of this protocol is obtainable using the emerging technology of XML Web Services. The accomplishment is entirely well-matched with the Federal Enterprise Architecture reference models and can be straightforwardly incorporated into existing E-Government systems. We consider our cross agency information sharing scheme can transform the circumstances where no one wants to share information to that condition where everybody wants to proactively share information by others, so that the mutual trust can be rebuild among different agencies, differences between agencies can be endured, get the wrong idea among agencies can also be reduced, inconsistency can be resolved, and efficient information sharing can be accomplished. With secure and effective information sharing the different agencies capability to forecast attacks and anticipate them can be extensively improved.

In this paper [13], author has presented a general idea of the predicament of securely sharing information among mutually-distrusting parties in a distributed system, beside with bearings of investigate toward solving the difficulty that

arise for attacking these problems, thinking of a number of alternative structures that observe the privacy vs. utility problem from different angles. Here author consider new mechanisms such as economic incentives to share data or discourage data leakage and a hybrid of code-splitting and secure multi-party calculation to make available a variety of assurances of confidentiality. We talk about and by examining both online social networks in particular and community-based review applications in wide-ranging, here they explain factors that should be taken into thoughtfulness when ability to information sharing policies with a focus on collaborative computation, how to incorporate these mechanisms into practical applications, including online social networks, a suggestion system based on user's requirements to a certain extent than identities, and a "personal information broker" that scrutinizes data leakage over time.

Here author [13] has also discussed mechanisms for enforcing such policies, with a focus on collaborative calculation beginning with the proposals of secure multiparty computation and computation tearing. In this paper author [13] propose that these mechanisms be enlarged with means to keep sensitive code hidden, and to make certain that two-way calculation is dependable and well-organized, and to quantitatively follow knowledge about private information that can be understand from the consequences of calculations.

In this paper [14], author has finding an issues related to sharing privacy protection in information in a distributed system consisting of autonomous entities, each of which holds a private database based on the assumption that all parties are honest or semi-honest. Semi-honest behavior has been widely adopted as the model for adversarial threats. However, it substantially underestimates the capability of adversaries in reality. In this paper [14], author has mainly focused on a threat space containing more powerful adversaries as a replacement for that easy and well-organized explanations can be extended to deal with malicious adversaries that includes not only semi-honest but also those malicious adversaries.

Distinctively they finding an issues to show simple solutions can be efficient if we 1) constrain the adversary goal to be weakly malicious, or 2) allow making a tradeoff between accuracy and privacy. Many expansions to their work stay alive including 1) extending the information sharing function from intersection to other operations and 2) dealing with multiple parties in the system, including dealing with correlated attacks from multiple adversaries. In particular, author has categorized malicious adversaries into two extensively subsisting subclasses called weakly malicious and strongly malicious adversaries. Here author has characterize a measure of privacy leakage for information sharing systems and recommend protocols that can efficiently and proficiently protect privacy against different kinds of malicious adversaries on a distributed system.

IV. PROPOSED METHODOLOGY

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 allowed
else session expires.
Step 19: User will show whether session expires or not.
If not expired then whether password valid or not.

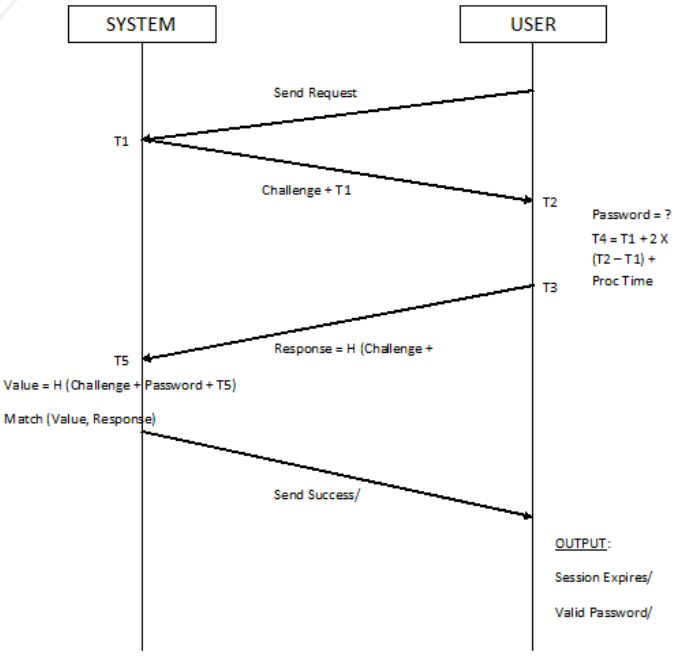

Figure 2. Architecture of CHAP Protocol

V. CONCLUSION

If the privacy-aware user modeling does unduly compromise users' perceived benefits of web personalization, then it fails to strike a good balance between privacy and personalization. Most of distributed applications that run on resource sharing platforms or in the clouds need access to heterogeneous, distributed and possibly private data. Usually, when such an access is required, it is the responsibility of the application developer to manage efficient access to all the data sources, and to integrate the data obtained from heterogeneous databases. Such a burden in the application development is not desired, and can be greatly reduced by using data services providing uniform access to distributed data.

REFERENCES

[1] W. Diffie and M. Hellman, "New directions in cryptography", in the IEEE Transaction on Information Theory, vol. 22,issue 6, (1976)November,pp.472-492.

[2] W.Stallings, "Cryptography and Network SecurityPrincipals and Practices", Pearson edition (India) Pvt.ltd, 4th Edition,(2009).

[3] Simpson, W. (Ed.), "The Point-to-Point Protocol (PPP)," The Internet Engineering Task Force, RFC 1661, July 1994.

[4] Yehuda Lindell and Benny Pinkas. Secure multiparty computation for privacy-preserving data mining. Cryptology ePrint Archive, Report 2008/197, 2008. http://eprint.iacr.org/

[5] C. Clifton, M. Kantarcioglu, X. Lin, J. Vaidya, and M. Zhu. Tools for privacy preserving distributed data mining, 2003

[6] Wang, Y. and Kobsa, A. (2009). Privacy-enhancing technologies. In Gupta, M. and Sharman, R., editors, Social and Organizational Liabilities in Information Security, pages 203–227. IGI Global

[7] Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu "Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 6, pp. 888 – 900, June 2013.

[8] Stephen S. Yau, Fellow, IEEE, and Yin Yin,"A Privacy Preserving Repository for Data Integration across Data Sharing Services", 2008.

[9] Kuijpers, Bart, Vanessa Lemmens, Bart Moelans, and Karl Tuyls. "Privacy Preserving ID3 over Horizontally, Vertically and Grid Partitioned Data." arXiv preprint arXiv:0803.1555, 2008.

[10] Gangrade, Alka, and Ravindra Patel. "Privacy Preserving Two-Layer Decision Tree Classifier for Multiparty Databases." International Journal of Computer and Information Technology (2277–0764) 1, no. 1, pp. 77-82, 2012.

[11] Shikfa, Abdullatif, Melek Önen, and Refik Molva. "Privacy-preserving content-based publish/subscribe networks", In Emerging Challenges for Security, Privacy and Trust, pp. 270-282. Springer Berlin Heidelberg, 2009.

[12] Liu, Peng, and Amit Chetal. "Trust-based secure information sharing between federal government agencies", Journal of the American society for information science and technology 56, no. 3, pp. 283-298, 2005.

[13] Mardziel, Piotr, Adam Bender, Michael Hicks, Dave Levin, Mudhakar Srivatsa, and Jonathan Katz. "Secure sharing in distributed information management applications: problems and directions", In Proceedings of the Annual Conference of the International Technology Alliance (ACITA). 2010.

[14] Zhang, Nan, and Wei Zhao "Distributed privacy preserving information sharing", In Proceedings of the 31st international conference on Very large data bases, pp. 889-900. VLDB Endowment, 2012.