ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

Privacy preserving in a secure network

Sandhya D. Patil[1], Prof. Nita M. Thakare[2]

Department of computer technology, priyadarshini College, Nagpur, India [1,2]

Abstract: This paper describes the problem of Privacy Preserving Data Mining (PPDM). Data mining is the process of extracting hidden information from the database. The current trend in business collaboration shares the data and mine results to gain mutual benefit. Privacy preserving data mining has become increasingly popular because it is allowing the sharing of private sensitive data for analysis purposes. It describes some of the common cryptographic tools and constructs used in several PPDM. An anonymous ID assignment technique is used iteratively to assign the nodes with ID numbers ranges from 1 to N. This technique enhances data that are more complex to be shared securely. The nodes are assigned with the anonymous ID with the help of a central authority.

Keywords: PPDM, anonymous id, privacy preservation, AIDA algorithm

INTRODUCTION

The anonymous communication plays a vital role in internet's popularity for both personal and business purposes.. The disadvantages of sharing private data are being studied in detail. Other available applications like searching of patient medical records, maintaining security about social networking, electronic voting and many more. To distinguish between anonymous communication and anonymous ID assignment, consider a situation where N parties wish to display their data, in N slots on a third party site, anonymous ID assignment method assigns N slots to the users whereas anonymous communication allows the users to conceal their identities. In our network the identities of the parties are known but not the original identity. In this paper we use an algorithm for sharing simple integer data which is based on secure sum algorithm. And reducing the problems occurred by newtons and strums theorem for applying long integer data n respective data to a particular extend.

Here we are going to implement an algorithm AIDA andwith this algorithm we are providing security to large amount of data by assigning a private key to a authorized user and a public key to an unthorised users. As explained above we are implementing an application like maintaining patient medical record, social networking. .

With the use of anonymous id assisgnment technique which makes information confidential we are using security algorithms with database management system to keep records of all hospitals.

RELATED WORK

Existing and new algorithms for assigning anonymous IDs are examined with respect to trade-offs between communication and computational requirements. suppose that access to the database is strictly controlled because data are used for certain experiments that need to be maintained confidential,which allows Alice directly to read the contents of the tuple breaks the privacy of Bob; the confidentiality of the database managed by Alice is violated once Bob has access to the contents of the database, without informing Alice and Bob know the contents of the tuple and the database respectively. Such functions are useful in data mining applications and also helps characterize the complexities of the secure multiparty computation. Our main algorithm will be based on a method for anonymously sharing simple data and results in methods for efficient sharing of complex data. So many applications are exists that require dynamic unique IDs for network.

The use of newtons and sturms algorithm minimizes the problems of an existing system but they are not going to implement a complex data structure, no doubt they are using secure sum function but still they are having data accessing problem as data goes on increasing day by day.

Every time they need to secure sum algorithm as data is increasing that increases the overhead of calculating sum and everytime display function of it. so it is directly affect on accessing and calculation of n data among various inputs with respect to their output. So to minimize this overhead we are going to implement an aida alogirithm with ecc curve that directly calculate the records of the data without using secure computation function and without using newtons and sturms theorems. That means we are going to exploring the three stages work into in only one step, which reduces overhead and saves times to calculate a frequent number of time secure sum function.

PROPOSED PLAN OF WORK

Our proposed work will be worked in four phases as follows:

Phase1: In this the system is dealing with implementation of different security algorithms and processing of data which is a communication module.

Phase 2: Creating an application to let the user sharing the data through secure channel and assignment of different IDs. we are going to implement data base connection.

Phase 3: This phase consists of the implementation and performance evaluation of the approach. Effectiveness of our propose approach will be measured in terms of accuracy. Evaluate its performance in terms of localizable rate, location error and computational overhead. That is number of users are going to sharing plus providing security.

Phase 4: we are analyzing how system works that is each users performance of quering to server.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

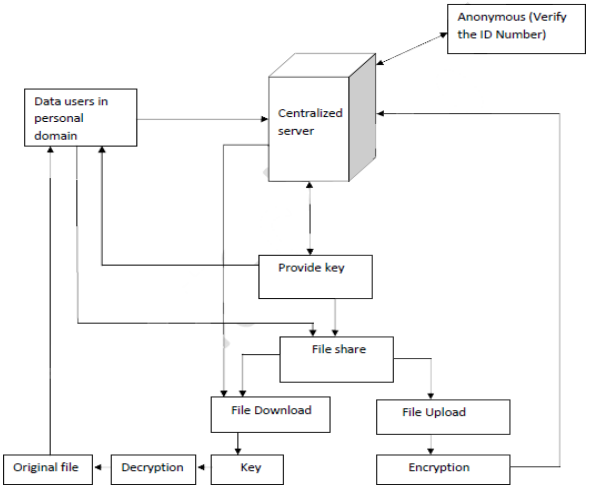

Fig.1 Simple working of a system

WORKING OF PROPOSED SYSTEM

we are implementing a system that is basically work on client server architecture. As shown in above figure the centralised server is a data central server that containing the information about the all medical records of the patient.The clients who want to access the information must be authorized themselves with a private key provided by the server to which the server provides private key.

After requesting from the client s server must show the current activity of the clients cpu like usage of cpu, how many times of request are coming from the client etc.

The server must also show the information about client like IP address of a client, cpu usage, requesting load of cpu etc.

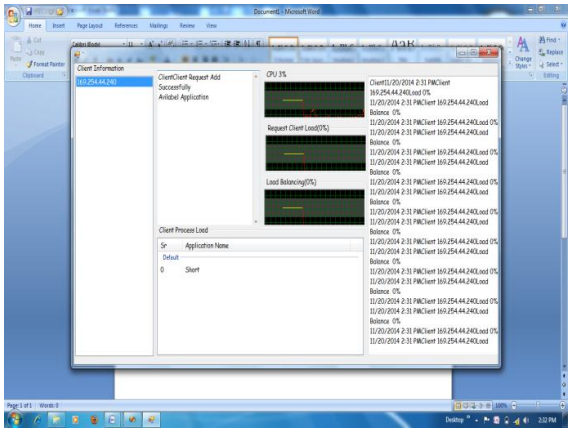

Fig. 2 information of client site server.

CONCLUSION

By using above method we are going to implementing a system that is work on aida algorithm with the use of ecc curve directly, and exploring the usage of ecc curve to accessing medical records. This paper isbasically used for a survey of medical patients for a particular disease. Acces is made easy for a particular patient with efficient and in a secure manner.

REFERENCES

[1] Sarbanes–Oxley Act of 2002, Title 29, Code of Federal Regulations,Part 1980, 2003.
[2] White Paper—The EssentialGuide toWeb AnalyticsVendor Selection,IBM [Online]. Available:ttp://measure.coremetrics.com/corem/getform/reg/wp-evaluation-guide
[3] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
[4] A. Friedman, R. Wolff, and A. Schuster, "Providing k-anonymity in data mining," VLDB Journal, vol. 17, no. 4, pp. 789–804, Jul. 2008.
[5] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A.Vaccarelli, "Seas, a secure e-voting protocol: Design and implementation,"Comput. Security, vol. 24, no. 8, pp. 642–652, Nov. 2005.
[6] D. Chaum, "Untraceable electronic mail, return address and digital pseudonyms," Commun. ACM, vol. 24, no. 2, pp. 84–88, Feb. 1981.
[7] Q. Xie and U. Hengartner, "Privacy-preserving matchmaking for mobile social networking secure against malicious users," in Proc. 9th Ann. IEEE Conf. Privacy, Security and Trust, Jul. 2011, pp. 252–259.
[8] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental Game."

BIOGRAPHIES

Prof. Nita M. Thakare, Priyadarshini Collegage of Engineering,Nagpur.
Teaching experience of 18 years, Phd. In computer environment.

Sandhya D. Patil, having teaching experience of 2 yrs. M.E. WCC.Priyadarshini college of Engineering Nagpur.