ISSN:0975-9646

# Mixnet for Anonymous Communication to Preserving Privacy in Hierarchical model networks

R.Srinivas[#1], Dr A. Yesu Babu[*2]

[#]*SSAIST, Surampalem*
*Andra Pradesh,India*

[*] *C.R.Reddy College of Engineering*
*Eluru,AP,INDIA*

*Abstract*— **Organizations of various types often collects, analyzes and disseminates data rapidly and accurately without exposing sensitive information to unauthorized or entrusted parties[14]. In such applications Anonymous communication is required to provide privacy to the data and nodes which contains this data. Communication anonymity means a particular message cannot be linked to any sender-receiver pair and no message is linkable to a particular sender-receiver pair. Sender anonymity prevents a particular message from being linked to a particular sender identity. Receiver anonymity prevents a particular message from being linked to a particular receiver identity.**

**Several Anonymous Communication Systems have been developed to achieve anonymity including Crowds , Herbivore, Mixminion and Tor. These technologies offer varying degrees of anonymity to protect the user's identity and provide privacy over a communication systems. The efficiency anonymous protocols depends strongly on a number of factors including: the number of anonymous users, how messages are routed, adversary knowledge and ability and other environmental factors for both the Internet and mobile ad hoc networks.**

**In hierarchical model to provide privacy to the data and data contents we proposed mixnet. Use of Mixnet improves the privacy in the network as well as provides anonymous communication**

*Keywords*— **Privacy, anonymous communication, Mix, Hierarchical Model, PPDM, anonymity**.

## INTRODUCTION

Many types of organizations must often collect, analyze and disseminate data rapidly and accurately without exposing sensitive information to wrong or entrusted parties.The data available to the public should not contain sensitive information. Before publishing data to the public personal identification number, ids, PAN numbers, cell phone number and other the attributes which reveals the personal identity need to be removed from the data. Even though this information is removed from the data still data is having some attributes which can be collectively used for identifying individuals. This set of attributes is called quasi set. If quasi set present in the data still there is a scope for individual identity.So in order to provide privacy to the individual, multidimensional k-anonymity is applied to the data before publishing the data. Not only providing privacy to the data we should also provide anonymity to the nodes which contains that.In the application nodes are not allowed to reveal the information from one another, so we should provide anonymous communication.

The process of privacy preserving leads to loss of information, this loss of information leads to loss of utility. Many attributes may need to be suppressed in order to preserve anonymity. In distributed databases privacy preservation allows us to compute useful aggregate statistics over the entire data without compromising the privacy of individual data. The participant sites may collaborate to prepare useful statistics and aggregates and in obtaining aggregate results.

Anonymity is also important for protecting user privacy in sensitive online forums involving sexual abuse, sexual conduct, religious beliefs, cultural issues, racial issues, harassment, and whistle blowing . Anonymity gives users a non-attributable channel to vent their benign or divisive opinions without fear of eventual identification and retribution.

The fundamental anonymity properties covered in the academic literature include sender, receiver, communications and location anonymity.For completeness, the unobservability property is also discussed.

A mix is the most extensively researched and implemented anonymous technology. The original mix was designed to make e-mails untraceable[16] . Other applications of a mix include secure electronic voting, anonymous telecommunications, and anonymous Internet communications. Subsequent mix variations protect against or avoid specific attacks and/or seek to boost performance in specific application domains. A representative mix is shown in Figure1.

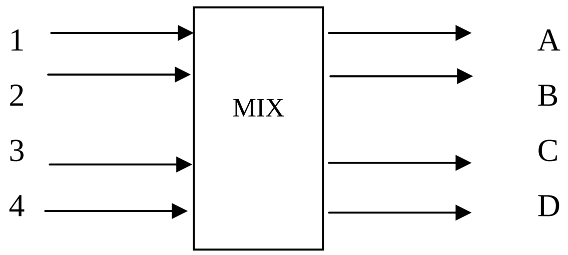
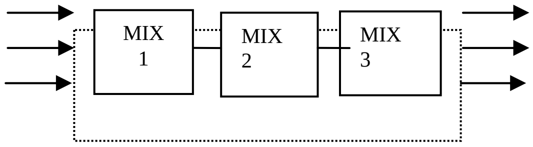
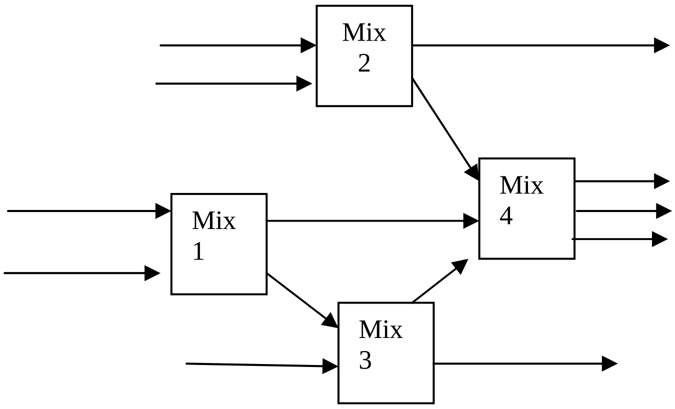


Fig. 1 Mixnet

Multiple mixes are connected together to form a mix topology and are called mixnets. The two main topologies are illustrated in Figure 2.



a.Cascades



b. Free route

Fig.2 Mix topology

Either of the mix topology is used in the hierarchical model to improve the privacy in data transmission and also to provide anonymous communication between sender and receiver.

Mixnet are useful for providing more privacy in network, these mix nodes are used in between the nodes of hierarchical model. While data is transferred between nodes through mixnet, the mixnet changes the order of the records received by reciver, so the reciver may know which decents containts what. The model is given in fig 3.

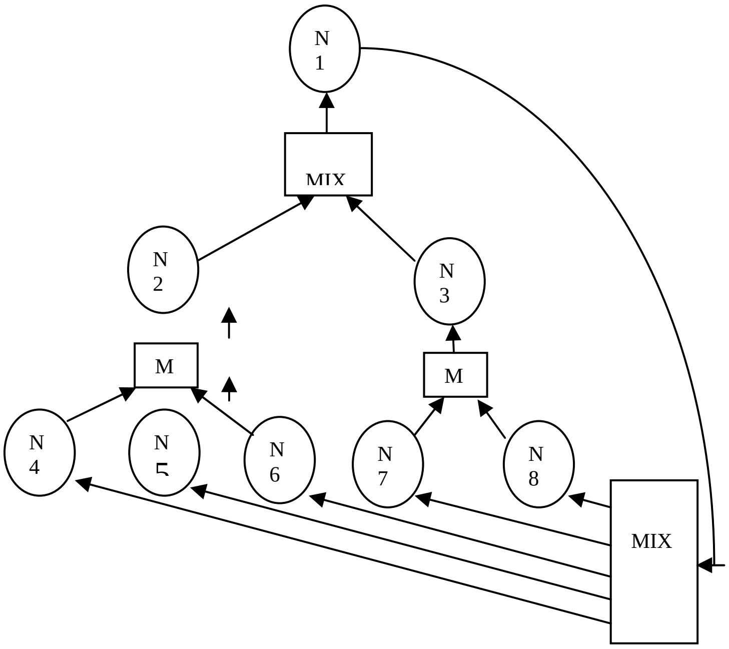


Fig3. Mixnet in hierarchical model

## II. METHODOLOGY

We assume that distributed databases contains horizontally and vertically partitioned data. One bit flag is added to each record in database available at sites. This flag is used to indicate whether the record is complete record or vertically partitioned record. To deliver the result to user, the data must be collected at one site. To collect data at one site first leader transmits its data to other nodes through mixnet. The records available at leader node are encrypted first except the primary key which is used for join operation if the data is vertically partitioned. If it is horizontally partitioned then all attributes are encrypted. These encrypted records are divided into several groups and these groups depend on the number of leaves. The data groups are transmitted to mixnet. This mixnet change the order of records to be delivered and forward these records to leaf nodes.

The leaf nodes receive the records and perform necessary operations and forwards to the next level through Mixnet.

The operations performed at leader and other nodes given below.

*Algorithm at leader site*

1. Wait until query has been received, once query is received it sends this query to all the other nodes in the network.
2. The leader node itself executes this query and from the query resultant it removes all the identifiers.
3. Identifier removed records are used for encryption except join attribute if the record is vertically partitioned and every other attribute is encrypted and this result is used to prepare the set and these sets are randomly send to the leaves in the hierarchical model and wait for receiving result from its decedents.
4. Once it receives the result, it uses decryption key inorder to decrypt the data from the decrypt data it removes the identifiers and it applies multidimensional k-anonymity for providing privacy to the sensitive information.
5. The result obtained from step 4 is published to the user.

*Procedure followed at non Leader site*

1. Wait for receiving query from leader node
2. The node itself executes this query and from the result it removes all the identifiers.
3. Identifier removed records are used for encryption except join attribute if the record is vertically partitioned and every other attribute is encrypted.
4. Once it receives vertically partitioned records from decedents apply join operation on records its vertically partitioned records and union operation on other records and the obtained result is forwarded in the network.

## III. CONCLUSION

In this application for providing privacy, data may be vertically and horizontally partitioned and stored at various sites. In order to get best results for research, data should be collected at one site to provide site anonymity and to provide privacy to information. We proposed the Hierarchal model to transfer partitioned distributed data. Once leader node receives data from all the nodes which contains the result of the query, then the leader node decrypts the data and publishes the data to the end user. The published data does not reveal identity of individual and provide site anonymity. The published data is useful for research and analysis.

## REFERENCES

1] Kristen LeFevre, David J.DeWitt, RaghuRamakrishnan: “Mondrian multidimensional k-anonymity” In ICDE, page 25,2006.

[2] Pawel Jurczyk,Li Xiong .”DObjects : enabling distributed data services for meta computing platform” In proc. Of the ICCS, 2008

[3] R. Srinivas et al.,. “Effective Bandwidth Utilization using Trusted LPEs in Anonymous Communication” *International Journal of Computer Applications (0975 – 888) Volume 47– No.7, June 2012*

[4] Wongil choi, Joonsuk ryu, Won young kim, Ungmo kim . “Simple data transformation method for privacy preserving data republication” IEEE 2009 : 978-1-4244-428-7109.

[5] Ren Xiangmin, Yang Jinf, Zhang Jianpei, Wang Kecho: ” Research on CBK(L,K)- anonymity algorithm” IJACT volume 3: number-4 may 2011.

[6] Latanya Sweeney: “ K- anonymity : A model for protecting privacy” IJUFKS 10(5) :2002; 557-570

[7] K. LeFevre, D.J.DeWitt, and R. Rama Krishna. “Incognito: Efficient full domain k-anonymity. In SIGMOD conference, pages 49-60,2005.

[8] R.J. Bayardo and R.Agrawal. “ Data privacy through optimal k-anonymity”, In Proc. 21st Intnl.Conf.Data Engg(ICDE),pages217-228,USA,2005.

[9] Ashwin Machanavajjhala , Johannes Gehrke, Daniel Kifer : “l-diversity: Privacy beyond k-anonymity” In Proc. 22nd Intnl. Conf.Data Engg.(ICDE),pages 24,2006

[10] Ninghui Li, Tiancheng Li, Suresh Venkatasubramanian:” t closeness : privacy Beyond k-anonymity and l-diversity” ,In ICDE, pages106-115,2007

[11] Pawel Jurczyk,Li Xiong : “Privacy preserving data publishing for horizontally partitioned databases” Technical Report TR-2008-013,EmoryUniversity,Math&CSDept,2008.

[12] R. Srinivas et al., Hierarchical Model for Preserving Privacy in Horizontally partitioned Databases” IJETTCSVolume2 Issue1 jan-feb-2013

[13] Guan, Yong, Xinwen Fu, and Riccardo Bettati, "An Optimal Strategy for Anonymous Communication Protocols," Proceedings of the 22nd International Conference on Distributed Computing Systems, College Station, TX, 2002.

[14] K Peng and F Bao”Trust management in privacy preserving information system “ IEEE 2010 8-1-4244-5540-9/10

[15]R. Srinivas et al.,. “Preserving Privacy in Horizontally Partitioned Databases Using Hierarchical Model” *IOSR Journal of Engineering May. 2012, Vol. 2(5) pp: 1091-1094*

[16] D. Chaum, BUntraceable electronic mail, return addresses, and digital pseudonyms Commun. ACM, vol. 24, no. 2, pp. 84–88,1981.