ISSN:0975-9646

Preserving Anonymity in Mixnet using AES Encryption Algorithm

M. Uma Devi, R.Srinivas, K.N.Bhargavi

CSE Department, SSAIST
KAKINADA, INDIA

Abstract **Data is one of the most important resources to organization and any loss or lack of access could lead to many problems, so the data should be transmitted with security. Although encryption was used to hide the contents of transmitted data, it does not hide the identity of the communicating parties and it does not prevent traffic analysis.Anonymity in a communication context, also known as untraceability, prevents tracing back from a receiver to the sender. So for providing anonymity one of the most efficient systems is MIXNET. The most important applications of Mixnets are in secure electronic voting, anonymous e-mail, anonymous telecommunications and anonymous internet communications .In e-voting protocols, a Mixnet anonymously communicates ballots from the voter to the electoral authority, hence providing ballot secrecy.**

In addition to presenting the existing Mixnet with cascade topology, this approach encrypts N messages using AES encryption which provides high confidentiality and permutes the data at each mixnode for providing anonymity. If N number of messages are encrypted by using AES encryption, then they will get permuted at each mixnode of the Mixnet until it reaches the nearest mixnode of receiver, then the data is decrypted using AES decryption algorithm and it is sent to corresponding N receivers.

***Keywords*— Data, Encryption, Anonymity, mixnode, AES, privacy, Mixnet**

I.INTRODUCTION

Data represents a repository for all information regarding business regardless of when it is started. Data is vital for business and it is required to find ways to protect it. Data security methods are essential for any organization, whether big or small. Now-a-days customers prefer to handle all their transactions online, so they want to make sure that their information is in safe hands. Security methods used are Data Encryption, Prevention of Access to Keys, Data Limitation, Online Data Backup and so on

Encryption means the conversion of plaintext or data into unintelligible form by means of a reversible translation based on a translation table or algorithms. That is, it does not hide the fact that some message was sent from or received by a particular site. Thus, if some location (or network node) A is sending and/or receiving a lot of messages to/from B, and if an adversary can monitor this fact, then even if the adversary does not understand what these messages mean, just the fact that there are a lot of messages between A and B reveals that and when they cooperate.

Anonymity means that it is untraceable who communicates with whom. The objective of anonymous communication is to show how to hide, in an efficient manner, the identity of users who transmit (or receive) a data to (or from, respectively) other sites in the network.A mixnet is a multistage system that uses cryptography and permutations to provide anonymity. Here we are providing anonymity by using the system called Mixnet.

i)DATA SECURITY METHODS

Planning to protect our data may be something that is easy to talk about yet very hard to implement. There are some strategies we need to use. These include:

a)Data Encryption:-To store sensitive information on a system that host locally, it is required to use encryption as a method of data protection. Having firewalls and passwords are good, but at times people can bypass all these and access our data. When encrypted, the data that an intruder can access will be in a form that they cannot understand and without an encryption key, this data is totally useless.

b) Data Limitation:-Storing a lot of data on the local system is not recommended. This is because in case of any calamity, everything will be lost. To be on the safe side, it is preferable to store only information that is necessary for business.

*c) Prevent Access to Keys***:-**Even if we protect our information using encryption, there is a chance that our own employees may wrongfully use the encryption key to access the data. Therefore the third data protection method should limit access to the keys. That is we need to store the keys in very few places to have a control on access.

*d) Use Online Data Backup***:-** One way to make our data secure is to keep it in a location that is separate from business. Enlist the services of a reliable cloud storage company that will make sure that our data is safe from external intrusion or unauthorized internal access.

ii)ANONYMITY

However, encryption does not hide all relevant information.For example, it does not hide the identity of the communicating parties. That is, it does not prevent traffic analysis. By using encryption we can hide the data but we can't hide the source id to the receivers. To hide the communicating party identities there is a need of anonymity.

Anonymity means that it is untraceable who communicates with whom. Anonymity in a communication context, also known as untraceability, prevents tracing back from a receiver to the sender. Sending the data only by using encryption means giving a chance for adversary to analyse the traffic regulations. An adversary's efforts might take the form of attempting to discover secret data, corrupting some of the data in the system.

iii) MIXNET

A Mixnet is a multistage system that uses cryptography and permutations to provide anonymity. A mix network consists of several interconnected stages, depending on the robustness of anonymity required.

Mixnet is the combination of different stages in which the sender will send the data to a stage called third party without knowing the receiver who actually is sending that data, but that data is sent by authenticated sender. Each stage performs mixing on its inputs, and the mixed batch is then forwarded to the next stage in the mixnet or directly to their destinations. A Mixnet may also contain faulty stages that may fail to conduct mixing operations, and thus not produce any output batches.

a) Mixnet Topologies

The interconnection of the stages determines the mixnet topology. There are two types of topologies of the mixnet, 1) cascade mixnet 2) a free-route mixnet[18], as illustrated in below Fig. (a) and (b), respectively

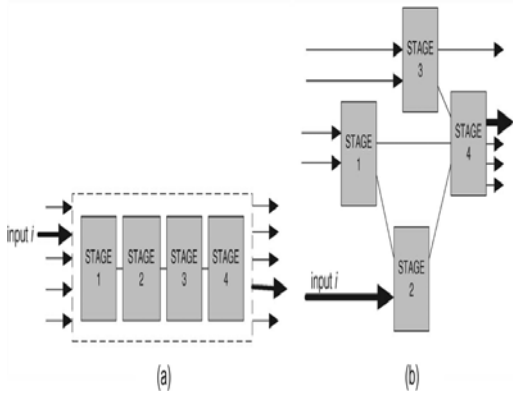

Fig1. Mixnet Topologies. (a) Cascade topology containing a fixed sequence of four stages. Anonymous communication path of five inputs includes all four stages. (b) Free-routing topology containing four interconnected stages. Each of five inputs can have from one to four stages included in communication path. For instance, an input i has stage 2 and stage 4 only in its anonymous path.

1) Cascade Topology For Anonymity

A cascade mixnet consists of stages connected in a fixed, sequential order in which all inputs traverses the same path as shown in above Fig.(a). The first stage in the cascade mixnet receives a batch of inputs, performs mixing, and then transfers in parallel the mixed batch to the connected second stage. The second stage then repeats mixing and forwarding, and the process continues until the final stage outputs the untraceable inputs.

A mixnet with cascade topology (cascade mixnet) consists of a fixed sequence of stages, leading to a single anonymous path for all senders communicating with receivers. Only the first stage of the cascade mixnet initiates mixing on all sender input batches. Since the path is already established from the input to the output of the mixnet, there is no requirement for explicit addresses for the stages to be included in the sender input. However, the stages in the cascade mixnet are interdependent, since a single stage in the mixnet can compromise or fail its operation

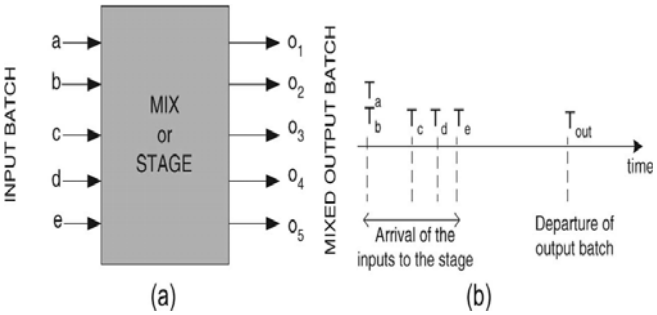

Fig 2.(a) Mixing by stage changes appearance of inputs and also removes order of arrival information. Output batch is a permutation of the transformed input batch. (b) Different times of arrival of inputs at the mix/stage and exit of mixed output batch.

In cascade mixnet the inputs arrive to the stage at different times, at last the outputs departure at the same time as shown in the above fig.2(b)

2) Free-Routing Topology for Anonymity

Free-route mixnet topology contains a number of anonymous paths with different number of stages. Because of the availability of a number of paths, the sender can choose any anonymous path. But if sender chooses any one path, if any of the stage fails, the sender again has to choose another path and re-initiate the communication.

In our proposed method we are using cascade mixnet topology only.

b) Attacks in mixnet:

In order to evaluate the security properties of a mixnet, adversary model can launch passive or active attacks on the mixnet. There are two types of attacks

a) Passive Attacks b) Active Attacks

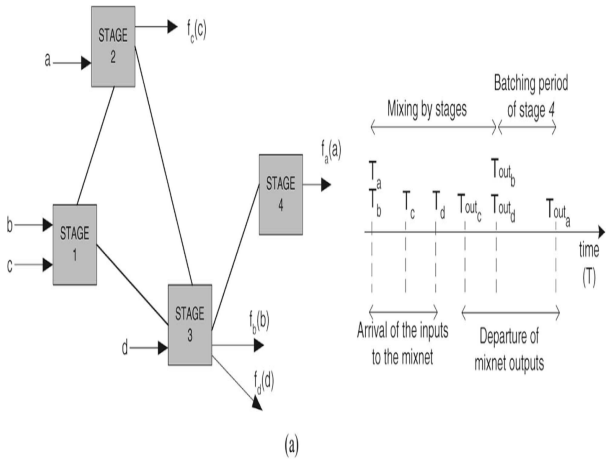

Fig 3 . Asynchronous batching in free-route mixnet with batch size threshold 2.

The passive attack can be performed by the adversary only if he analyze a batch, inorder to trace any input in that batch while for an active attack the adversary must control the inputs in the batch.

*a) Passive Attacks***:** The adversary performs traffic analysis in order to conjecture the correspondence between the N inputs and the N outputs in a batch. By observing the inputs to the cascade mixnet, the adversary may get time and appearance information. But after mixing is initiated in the first stage, for tracing an input to the corresponding output, the adversary is forced to choose from the N outputs in the batch.

*Solution***:** By increasing the batch size, robustness against this attack can be achieved.

b) Active Attacks: In an active attack, an adversary may control some compromised stages and use them to trace an input passing through. In order to break the anonymity of the cascade mixnet, an adversary must control at least a threshold number of S stages.

Solution: Hence, by increasing the threshold S, as threshold value depends upon the number of stages N in a cascade mixnet, robustness can be improved against attacks on anonymity.

iv) AES ENCRYPTION

AES (Advanced Encryption Standard) is a widely adopted symmetric encryption scheme used, for instance, to secure electronic communication and messages. AES – as its name implies - has been the outcome of standardization and evaluation process which took years to select from the best encryption algorithms. In the AES implementation of Rijndael the algorithm operates on 128 bits block ciphers, and comprises key lengths of 128, 192 and 256 bits. It is common to refer to the symmetric key AES encryption standard as AES-128, AES-192 and AES-256 depending on the key strength. AES operates on a 4×4 array of bytes, termed the state (versions of Rijndael with a larger block size have additional columns state).For encryption, each round of AES consists of four stages:

- AddRoundKey
- SubBytes
- ShiftRows
- MixColumns

The final round replaces the MixColumns stage with another instance of AddRoundKey.

II PROPOSED METHOD

Our idea is to refine this existing approach by implementing the Mixnet using AES encryption & Decryption by permuting the messages each time at mixnodes with cascade topology.

1. The N-number of messages are sent from N number of senders to N number of receivers and while sending the messages the address or ID of the receiver is concatenated with each message(M, id) where M is message and id is identity of receiver

2. Then that concatenated message is encrypted using AES encryption algorithm. In our proposed method we prefer AES as it is safe and secured. It can be performed in a variety of settings (PCs of various architectures, smart cards, hardware implementations) and feasible in limited environments .If N=3 then 3 messages are encrypted. If N value increases anonymity increases and Robustness against attacks also increases.

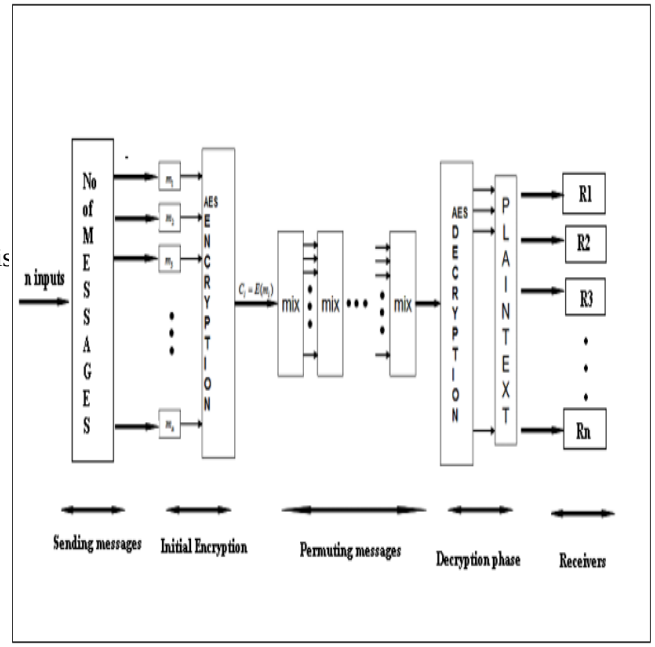

Fig 4 .Providing Anonymity using Mixnodes b/w senders and Receivers

3. The Encrypted message i.e the cipher texts will be forwarded to the first mixnode. The first mixnode then permutes the data and then send the data to the second mixnode. Now the second mixnode permutes data and then send the data to the third mixnode and so on.

4.If there are x number of mixnodes .The N-cipher texts from the xth mixnode which is the nearest mixnode to the receiver will be decrypted using AES algorithm and sent to receivers.

5. The receivers will receive the correct message accordingly sent by the senders. Similarly if there are more number of mixnodes the anonymity and robustness against attacks also increases. So the number of messages and number of mixnode value depends upon the threshold value. If there are more number of messages and more number of mixnodes the adversary cannot attack.

Inputs:-
Enter No. of clients wish to send: 3
Enter 3 Messages:
Client 1: Srinivasgaru
Client 2: Uma
Client 3: Bhargavi
Outputs:-
Encrypted string isB1H8pg+hRIgdnK2mdMB4Dg==
Encrypted string isAxAiodb2nuGZ/qPf2MdZdA==
Encrypted string isUrYOOGtIR01gJobHSwgzYw==
After first PermutationUrYOOGtIR01gJobHSwgzYw==
After first PermutationB1H8pg+hRIgdnK2mdMB4Dg==
After first PermutationAxAiodb2nuGZ/qPf2MdZdA==
After Second PermutationB1H8pg+hRIgdnK2mdMB4Dg==
After Second PermutationUrYOOGtIR01gJobHSwgzYw==
After Second PermutationAxAiodb2nuGZ/qPf2MdZdA==
Receiver 1: Srinivasgaru
Receiver 2: Uma
Receiver 3: Bhargavi

III.CONCLUSION AND FUTUREWORK

In our proposed method, AES Encryption and Decryption algorithm is used for encrypting the messages. N number of messages is permuted at each mix nodes by using cascade mixnet topology so that confidentiality, anonymity and robustness increase. In future work, apply AES encryption algorithm to different topologies and test the results for better accuracy.

REFERENCES

[1] A. Young and M. Yung, Malicious Cryptography: Exposing Cryptovirology New York: Wiley, 2004.

[2] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, BProtocols using anonymous connections: Mobile applications,[in Proc. Security Protocols,1997, pp. 13–23.

[3] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, BEnhancing wireless location privacy using silent period, in Proc. IEEE Wireless Communications Networking Conf., 2005.

[4] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, Universal re-encryption for mixnets, in Proc. RSA Conf. Cryptographers'Track, 2004, pp. 163–178.

[5] J. Raymond, BTraffic analysis: Protocols, attacks, design issues and open problems, in Proc. Designing Privacy Enhancing Technologies Workshop, 2001, pp. 10–29.

[6] Free haven project bibliography. [Online].Available: http://www.freehaven.net/anonbib/date.html

[7] O. Berthold, A. Pfitzmann, and R. Standtke, BThe disadvantages of free mix routes and how to overcome them,in Proc.Anonymity, 2001, pp. 30–45.

[8] *en.wikipedia.org/wiki/Advanced_Encryption_Standard*

[9] M. Jakobsson and A. Juels, An optimally robust hybrid mix network,in Proc. 20th Annu. ACM Symp. Principles Distributed Computing (PODC 2001), 2001, pp. 284–292.

[10] R. Dingledine,M. J. Freedman, D. Hopwood, and D. Molnar, BA reputation system to increase MIX-net reliability,in Proc. Information Hiding Workshop, 2001pp. 126–141.

[11] C. Diaz and A. Serjantov, BGeneralizing mixes, in Proc. Workshop on Privacy Enhancing Technologies, 2003, pp. 18–31.

[12] *www.hexistor.com/data-security/secure-your-data-using-these-data-security*

[I3]M. G. Reed, P. F. Syverson, and D. M. Goldschlag. Anonymous connections and onion routing. In *IEEE Symposium on Security and Privacy*, Dec. 1997.

[I4] M. G. Reed, P. F. Syverson, and D. M. Goldschlag. Anonymous connections and onion routing. *IEEE Journal on Se-[ecredAreas in Communications*, 16(4):482494, May 1998.

[15] M. Reiter and A. Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*,1(1), June 1998.

[I6] D. B. S. Basagni, K. Herrin and E. Rosti. Secure pebblenets.In *MobiHoc '01*. pages 156163,2001.

[I7] R. Sivakumar, P. Sinha, and V. Bharghavan. Cedar: Acore-extraction distributed ad hoc routing algorithm. *IEEE Journal on Selected Areas in Communications*, 17(8): 1454-1465, Aug. 1999.

[I8] Krishna Sampigethaya, Student Member IEEE, and Radha Poovendran, Senior Member IEEE A Survey on Mix Networks andTheir Secure Applications