ONION SLEEVE ROUTING ALGORITHM

Prajna P Shetty[1], Shruthi Kumari M.L[2], Sukhada V.K[3], BhavyaRaj[4], Sindhu Venkatesh[5]

[1,2,3,4,5] Department of CSE, K.V.G.College of Engineering, Sullia, VTU Belgaum India.

ABSTRACT

Communication is the god given gift that enables intellectual and cultural exchange and builds up our competence in social behaviour. The internet has taken communication to unimaginable attitudes. Most security concerns focuses on preventing eavesdropping that is outsiders listening in on electronic conversions. But encrypted messages can still be tracked revealing who is talking to whom. This tracking is called as traffic analysis and may reveal sensitive information. As an initial step towards ensuring a secured communication we have chosen our paper as Onion Routing in LAN. First it securely establishes the connection using switches. To ensure the security well known networking and Public key Cryptographic techniques are utilized. Here the identities of the sender and the receiver are hidden by an onion structure, which is cryptographically layered data structure that defines the route through the onion routing network. After the route is established by making the entries into the routing table, the data is transmitted over the channel, which is repeatedly encrypted or decrypted using the passive as well as active modes, for high level security. Once the data is transferred the connection is destroyed. Using symmetric and asymmetric cryptosystems at different levels enhances further security. Though there are many alternative solutions such as anonymizer and crowds, Onion routing provides the efficient way of protection, which has been implemented.

Keywords: *Active, AES, Intermediate Node,Onion Router, Passive.*

I. INTRODUCTION

Onion routing is a technique for secure communication over a computer network. Messages are repeatedly encrypted or decrypted and then sent through several network nodes called onion routers[1]. This prevents these intermediate nodes from knowing the contents of the original one.The idea of onion routing is to protect the message sent from sender to receiver. Onion routing accomplishes this according to the principle of Chum's mix [2] cascades: messages travel from source to destination via a sequence of proxies ("onion routers"), which re-route messages in an unpredictable path. To prevent an adversary from eavesdropping on message content, messages are encrypted between routers.

A routing onion (or just onion) is a data structure formed by 'wrapping' a plain text message with successive layers of encryption or decryption using active and passive modes[3]. If active, then it has 4 jobs such as receiving the encrypted or decrypted text, decrypting to original text, encrypting it once again and forwarding it to next intermediate node. If so it is passive, then it will receive encrypted or decrypted text, encrypt it once again and forward it. Finally at the receiver it will decrypt until original message is obtained. An intermediate node is traditionally called a node or router.

The advantage of onion routing is that it is not necessary to trust each cooperating router[4]. This is because each router in an Onion Routing network accepts messages, encrypts/decrypts them, and transmits to another intermediate node. An attacker with the ability to monitor every onion router in a network might be able to trace the path of a message through the network, but an attacker with more limited capabilities will have difficulty even if he or she controls routers on the message's path.Onion Routing is a flexible communications infrastructure that is resistant to both eavesdropping[5] and traffic analysis. Onion routing accomplishes this goal by separating identification from routing. Connections are always anonymous, although communications need not be. Onion routing can be used by a variety of unmodified Internet applications by means of proxies or by modifying the network protocol stack on a machine to be connected to the network.

II. RELATED WORK

Author here contributes the detailed specification of the implemented onion routing system, a vulnerability analysis based on this specification, and performance results. Onion routing provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. Unmodified Internet applications can use these anonymous connections by means of proxies. The proxies may also make communication anonymous by removing identifying information from the data stream. Onion routing has been implemented on Sun Solaris 2.X with proxies for Web browsing, remote logins and e-mail[1].

People require privacy when doing transaction via Internet connection. For example, some people do not want other people to know what web page they request. Anonymous cash is not anonymous anymore if the channel used for the connection identifies the identity of the participating entities. Email users sometimes want to hide their email addresses. These days, the Internet does not really care about privacy. Encryption is provided to protect privacy, but it only protects the content of a transaction. Thus an eavesdropper can still learn the IP addresses of the internet users to infer their identities. Special networks, called the anonymity network, were created to protect privacy, especially the identities of the entities participating in a communication via Internet connections. This paper discusses probabilistic analysis of the anonymity provided by anonymity networks, namely Onion Routing, by using a model-checker tool called PRISM[2].

Onion routing is an infrastructure for private communication over a public network. It provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. Onion routing's anonymous connections are bidirectional, near real-time, and can be used anywhere a socket connection can be used. Any identifying information must be in the data stream carried over an anonymous connection. An onion is a data structure that is treated as the destination address by onion routers; thus, it is used to establish an anonymous connection. Onions themselves appear different to each onion router as well as to network observers. The same goes for data carried over the connections they establish. Proxy-aware applications, such as Web browsers and e-mail clients, require no modification to use onion routing, and do so through a series of proxies. A prototype onion routing network is running between our lab and other sites. This paper describes anonymous connections and their implementation using onion routing. This paper also describes several application proxies for onion routing, as well as configurations of onion routing network[3].

Providing anonymity for users on the Internet is a very challenging and difficult task. Currently there are only a few systems that are of practical relevance for the provision of low-latency anonymity. One of the most important to mention is Tor which is based on onion routing[4]. Practical client usage of Tor often leads to delays that are not tolerated by the average end-user, which, in return, discourages many of them from using the system. In this paper they propose new methods of path selection that allow performance-improved onion routing. These are based on actively measured latencies and estimations of available link-wise capacities using passive observations of throughput. They evaluate the proposed methods in the public Tor network and present a practical approach to empirically analyze the strength of anonymity certain methods of path selection provide in comparison to each other.

This paper presents a novel use of Elliptic Curve Arithmetic[5] to improve circuit construction in onion routing anonymity networks. The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead. Compared to previous designs, this algorithm provides practical forward secrecy and leads to a reduction in the required amount of authenticated directory information. In addition, it requires significantly less computation and communication than the previous designs. These properties suggest that approach is a practical way to allow anonymity networks to scale gracefully.

They consider it using trust information to improve the anonymity provided by onion-routing networks. In particular, they introduce a model of trust in network nodes and use it to design path-selection strategies that minimize the probability that the adversary can successfully control the entrance to and exit from the network. This minimizes the chance that the adversary can observe and correlate patterns in the data flowing over the path and thereby deanonymize the user. They first describe the general case in which onion routers can be assigned arbitrary levels of trust. Selecting a strategy can be formulated in a straightforward way as a linear program, but it is exponential in size. They thus analyze a natural simplification of path selection for this case. More importantly, however, when choosing routes in practice, only a very coarse assessment of trust in specific onion routers is likely to be feasible. Therefore, they focus next on the special case in which there are only two trust levels. For this more practical case identify three optimal route-selection strategies such that at least one is optimal, depending on the trust levels of the two classes, their size, and the reach of the adversary. This can yield practical input into routing decisions. They set out the relevant parameters and choices for making such decisions[6].

Communication is the god given gift that enables intellectual and cultural exchange and builds up our competence in social behaviour. The internet has taken communication to unimaginable attitude. Most security concerns focuses on preventing eavesdropping that is outsiders listening in on electronic conversions. But encrypted messages can still be tracked revealing who is talking to whom. This tracking is called as traffic analysis and may reveal sensitive information. It is an initial step towards ensuring a secured communication. Onion routing is a flexible communication infrastructure that is resistant to both eavesdropping and traffic analysis. The paper is two-fold. First it securely establishes the connection. To ensure the security well known networking and Public key Cryptographic techniques are utilized. Here the identities of the sender and the receiver are hidden by an onion structure, which is cryptographically layered data structure that defines the route through the onion routing network. After the route is established by making the entries into the routing table, the data is transmitted over the channel, which is also repeatedly encrypted. Once the data is transferred the connection is destroyed. Using symmetric and asymmetric cryptosystems at different levels enhances further security. Though there are many alternative solutions such as anonymizer and crowds, Onion routing provides the efficient way of protection, which has implemented[7].

III. PROPOSED METHODOLOGY

This project Onion Routing is for Local Area Network. The project comprises of three modules.

- Module I: Designing the encryption algorithm
- Module II: Connection Establishment.
- Module III: Data transfer.

The first step to implement onion routing is to design the encryption algorithms. Different algorithms are used for connection establishment and data transfer.

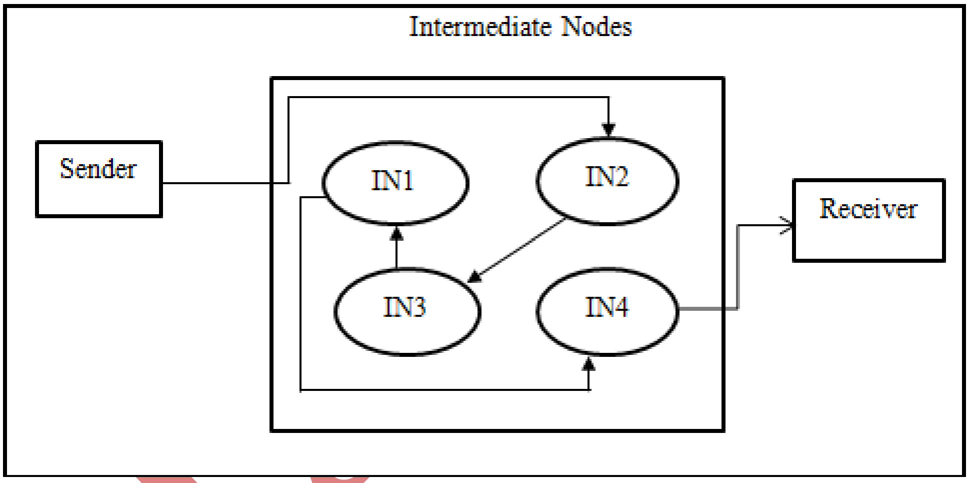


Fig.1: Architectural Design

For connection establishment Advanced Encryption Standard (AES) algorithm is the standard public key cryptographic algorithm and the cipher text cannot be decrypted easily because in AES algorithm the process of decryption is not an inverse process of encryption. The encryption and decryption message are generated using private key. The admin is responsible for assigning key for every particular intermediate node.

Module II:

The second step is the connection establishment.To explain the connection establishment let as consider the following local area network. Here U1, U2 are sender and receiver. P1, P2 and P3 are intermediate nodes. The intermediate nodes are also called as routers. This perform encryption and decryption phenomenon. The connection is established using switch and cables. In order to perform the secure communication the route to be found first .i.e., the path to be followed from sender to receiver and the addresses of the intermediate nodes is to be set. Then a message is passed from sender to intermediate node as per the path set by the admin. This message is then encrypted or decrypted in each intermediate node as per its secret key using AES algorithm in each intermediate node. It is then passed to the next intermediate nodes as per the path is set until it reaches the receiver.

Module III:

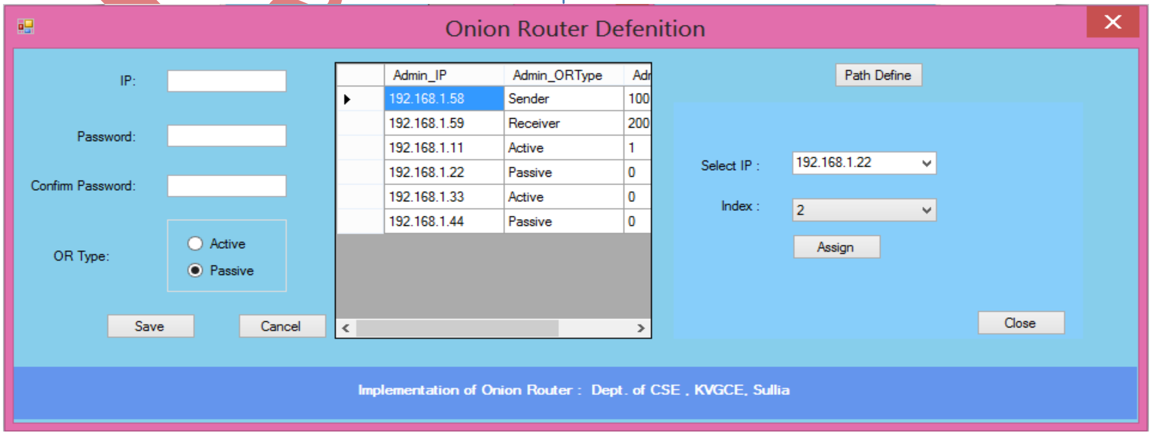
After the connection is established the message is passed over the path, which is encrypted or decrypted as per the modes specified by the admin (active/passive). Here presented a protocol called Onion Routing. The purpose of Onion Routing is to provide secure communication. To achieve this goal, Onion Routing uses Public Key Encryption to put multiple layers of encryption/decryption around the original data packet, thus creating an object called an onion. This onion will follow a specific route through the network, and at each route an encryption or decryption may take place as per admin has set the path. Once the message reaches its destination it will have been reduced to the original data packet by the receiver and no router will ever know the full path travelled by the onion and also no outside observer will be able to follow an onion while it is travelling through network,the communication becomes completely anonymous.

Routing onions are data structures used to create paths through which many messages can be transmitted. Admin is the head of a transmission selects a number of intermediate nodes at random and this intermediate nodes does encryption and decryption (active mode) or only encryption (passive mode) using its private key and instructing it which intermediate node will be next in the path. Thus, it provides a layered structure known as multi-layer structure. At the receiver, it uses AES algorithm to perform encryption or decryption as per the previous defined intermediate node by the admin. Thus, original message is obtained without any data mismatch or data misuse. It is completely secure system.

IV.EXPERIMENTAL RESULTS

In these experimental results,there are four modules. They are Admin module, Sender module, Intermediate Node module and Receiver module.

4.1 Admin form



Onion Router Defenition

IP:

Password:

Confirm Password:

OR Type: ○ Active ● Passive

	Admin_IP	Admin_ORType	Adr
▶	192.168.1.58	Sender	100
	192.168.1.59	Receiver	200
	192.168.1.11	Active	1
	192.168.1.22	Passive	0
	192.168.1.33	Active	0
	192.168.1.44	Passive	0

Select IP : 192.168.1.22

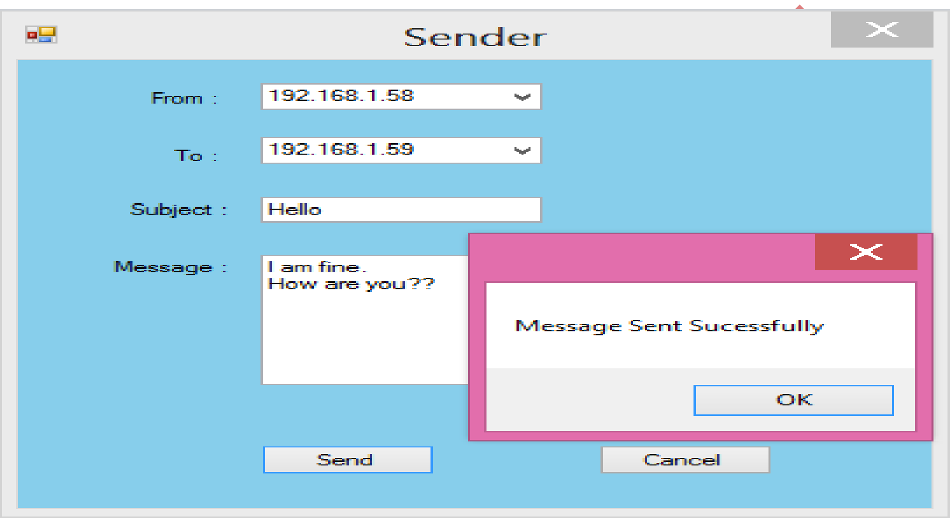
Index : 2

Implementation of Onion Router : Dept. of CSE , KVGCE, Sullia

Fig.2: Admin form

Here admin set IP address for sender, intermediate nodes and receiver. Then admin set the private key for all those forms. Select the OR type it may be active or passive, So the intermediate nodes here can be either passive or active.Here path define is used to select the paths for intermediate nodes by specifying theIP address and to which intermediate node the message should be passed first and to which node next is done by specifying in the index of this form .

4.2 Sender form



Sender

From : 192.168.1.58

To : 192.168.1.59

Subject : Hello

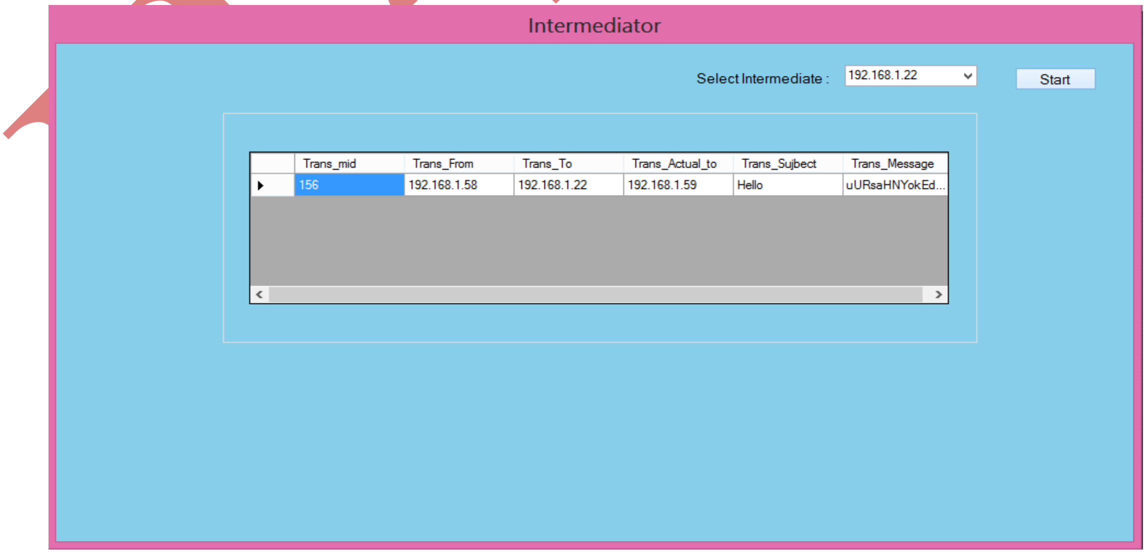
Message : I am fine.
How are you??

Message Sent Sucessfully

Fig.3: Sender form

In this formIP address for sender and receiver is given and then must give subject for the message that is sent from this sender to receiver through the intermediate nodes.

4.3 Intermediate nodes form



Intermediator

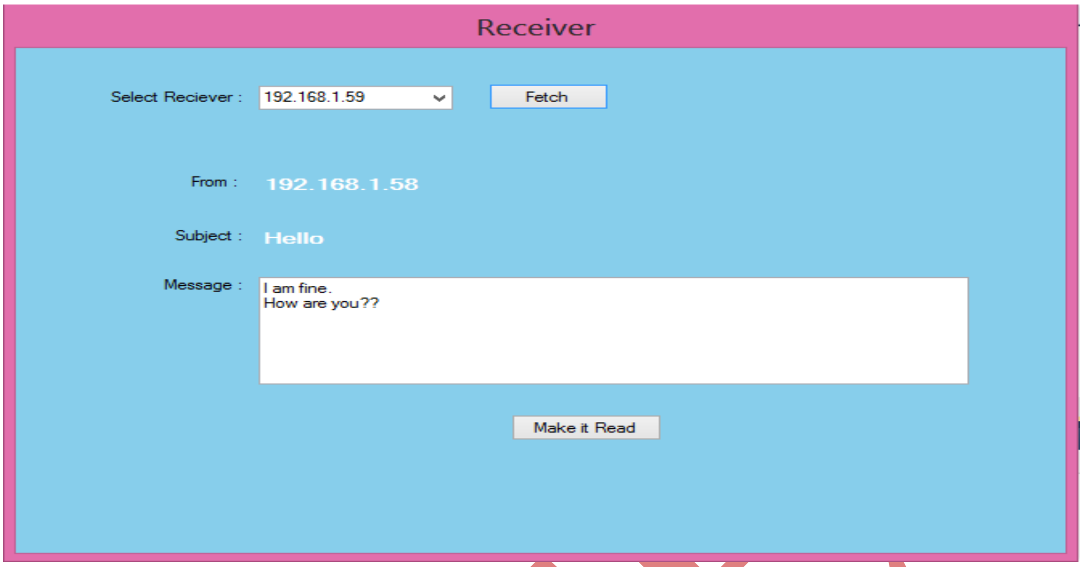
Select Intermediate : 192.168.1.22

	Trans_mid	Trans_From	Trans_To	Trans_Actual_to	Trans_Sujbect	Trans_Message
▸	156	192.168.1.58	192.168.1.22	192.168.1.59	Hello	uURsaHNYokEd...

Fig.4:Intermediate nodes form

Here in this form there is a start button, whenbutton is clicked the encrypted message from the sender is received.Andthere can be any number of intermediate nodes

4.4 Receiver form


Receiver

Select Reciever : 192.168.1.59

From : 192.168.1.58

Subject : Hello

Message : I am fine.
How are you??

Fig.5: Receiver form

In this form there is a fetch button which is used to get the message that has been sent through the intermediate nodesfrom the sender, there is a make it read option for erasing the previous messages**.**

V. PERFORMANCE ANALYSIS

Performance Analysis gives clear idea of Security,Speed and Timebut this project mainly focus on security as our objective is to give high level of security.Onion routing (OR) is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted/decrypted and then sent through several intermediate nodes .This prevents intermediate nodes from knowing the contents of the message. A routing onion (or just onion) is a data structure formed by 'wrapping' a plaintext message with successive layers of encryption/decryption using its secret key in each intermediate node.If there is end-to-end encryption/decryption between the sender and the recipient, then not even the last intermediate nodes can view the original message; this is similar to a game of 'pass the parcel'. An intermediate node is traditionally called a node or router. The Onion Sleeve Routing Algorithm is mainly Focus on providing high level of security. Here we provide multi layered protection it mean combination of both Active and Passive.

Table 1 : Comparison of AES and DES on basis of security

Plain	Original (cycles)	Rounds	Minimum Rounds	Time (cycles)
DES	1600	32	20	1000
AES (Rijndael)	1276	10	8	1021

From above table, we can conclude that this project Onion Sleeve Routing Algorithm provides better security than other existing system. It provides multi-layered protection. Hence it more secured when compared to previous approach. The elapsed time between the end of an inquiry or demand on a computer system and beginning of a response.For example, the length of the time between an indication of the end of an inquiry and the display of the first character of the response at a user terminal.

There is also the concept of perceived response time, which is the time a user senses as the beginning of input and the end of the response. It is actually possible for perceived response time to be too fast. Response time of this project Onion Sleeve Routing algorithm is 0.137seconds. When compare to existing system it has response time of 0.267seconds. Thus, our project has better response time compared to existing system.

Round-trip time (RTT), also called round-trip delay, is the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again. The source is the computer initiating the signal and the destination is a remote computer or system that receives the signal and retransmits it.

The result depends on various factors including:

- The data transfer rate of the source's network connection
- The nature of the transmission medium (copper, optical fibre, wireless or satellite)
- The physical distance between the source and the destination
- The number of nodes between the source and the destination
- The amount of traffic on the LAN (local area network) to which the end user is connected
- The number of other requests being handled by intermediate nodes and the remote server
- The speed with which intermediate nodes and the remote server function
- The presence of interference in the circuit.

Round Trip Time of this project is 0.448.seconds whereas previous existing system has 0.737seconds of RTT. Thus, project has better round trip time.Congestion, in the context of networks, refers to a network state where a node or link carries so much data that it may deteriorate network service quality, resulting in queuing delay, frame or data packet loss and the blocking of new connections. In a congested network, response time slows with reduced network throughput. Congestion occurs when bandwidth is insufficient and network data traffic exceeds capacity.

Data packet loss from congestion is partially countered by aggressive network protocol retransmission, which maintains a network congestion state after reducing the initial data load. This can create two stable states under the same data traffic load - one dealing with the initial load and the other maintaining reduced network throughput.

Onion Sleeve Routing Algorithm has a mean congestion time of 0.176 seconds. While previous existing system has mean congestion time of 0.237 seconds. So it has far good improvement over previous existing system. Thus, this project provides better response time, round trip time and mean congestion time.The performance of the algorithm is measured in terms of the speed, i.e., number of cycles required for the completion of the function. The speed of the algorithm can be characterized by measuring the time required for key scheduling, encryption and decryption

Table 2: Comparison of AES and DES with respect to speed

Speed			Key Setup	
Plain	Encrypt (cycles)	Decrypt (cycles)	Encrypt	Decrypt
DES	1600	1580	4780	5548
AES (Rijndael)	1276	1276	17742	18886

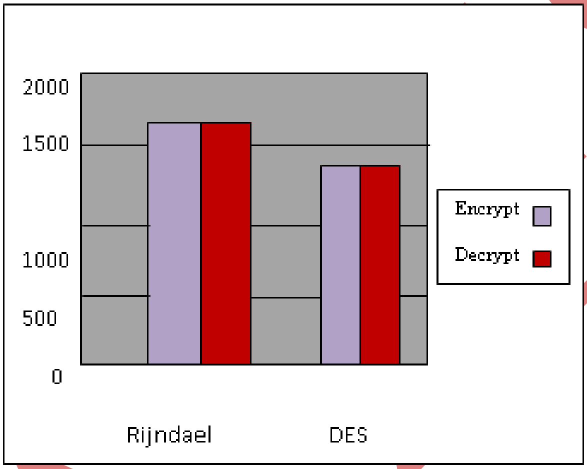


Fig. 6: Comparison of AES and DES with respect to speed

Thus,from above table and graph, we can conclude that speed of this project in comparivetely better to other existing system.This project Onion Sleeve Routing has got better security, time, and speed when compared to all other existing system.

VI. CONCLUSION

The purpose of Onion Routing is to provide the security to the message communicating over a network. In particular, it will hide the message from hacker by wrapping it with encrypted/decrypted data. Any outside observers will not be able to know what the actual message is. To achieve this goal, Onion Routing uses Advanced Encryption Standard to perform encryption and decryption phenomenon. This message will follow a specific route through the network, and at each route a layer of encryption/decryption takes place. Once the message reaches its destination it will have been reduced to the original data packet using private key of receiver. Since no outside observer will be able to follow a message while it is travelling through the network, the communication is completely secure.

REFERENCES

[1] Kaviya K.,*"Network Security Implementation by Onion Routing Information and Multimedia Technology"*, 2009.

[2] Panchenko A, Renner J.,*"Path Selection Metrics for Performance-Improved Onion Routing, Applications and the Internet"*, 2009.

[3] Adithia, M.,"Probabilistic Analysis of Onion Routing Networks Using PRISM, Informatics and Computational Intelligence (ICI)", 2011.

[4] Reed M.G, Syverson. P.F, Goldschlag, D.M., *"Anonymous connections and onion routing"*, 1998.

[5] Zhang Chaoyang., *"Elliptic Curve Arithmetic in onion routing anonymity networks"*,2011.

[6] Syverson P.F, Goldschlag D.M, Reed M.G., *"Anonymous connections and onion routing Security and Privacy"*,1997.

[7]Johnson A,Syverson P., *"More Anonymous Onion Routing Through Trust Computer Security Foundations Symposium"*,2009.

AUTHOR DETAILS

	Prajna P.Shetty has received Bachelor of Degree in Computer Science and Engineering from K.V.G College of Engineering, Sullia, which is affiliated to VTU Belgaum, India in 2014 (E-mail:prajnapshetty.92@gmail.com). Has done many researches on network basis. This is presented paper on this project in National Level Tech Fest held at K.V.G. College of Engineering, Sullia. Has keen interest in Computer Network and Security, Wireless communication Network and 3G.
	Miss Shruthi Kumari M.L., a B.E graduate in Computer Science And Enginnering from K.V.G. College of Engineering Sullia, VTU University Belgaum, Karnataka State, India. (E-mail:shruthigwd17@gmail.com) . Interested in the field of Resaearch and Development based on Computer Networks. Presented paper on this topic in National Tech Fest held at K.V.G. College of Engineering Sullia.
	Miss Sukhada V.K., a B.E graduate in Computer Science And Enginnering from K.V.G. College of Engineering Sullia, VTU University Belgaum, Karnataka State, India. (E-mail:siri.jazz@gmail.com) . Interested in the field of Resaearch and Development based on Wireless Communication And Mobile Computing. Presented paper on this topic in National Tech Fest held at K.V.G. College of Engineering Sullia.

	Miss BhavyaRaj, a B.E graduate in Computer Science And Enginnering from K.V.G. College of Engineering Sullia, VTU University Belgaum, Karnataka State, India. (E-mail:bhavyarajpallathadka@gmail.com). Interested in the field of Resaearch and Development based on C# and .NET. Presented paper on this topic in National Tech Fest held at K.V.G. College of Engineering Sullia.