Anonymous Communication System based on Onion Routing

Manish Dhankani
B.E. Comp Engineering
VES Institute of Technology

Abhishek Dhameja
B.E. Comp Engineering
VES Institute of Technology

Surendrakumar Darda
B.E. Comp Engineering
VES Institute of Technology

Dimple Bohra
Comp Engineering Dept.
VES Institute of Technology

ABSTRACT
Communication is one of the most important medium through which people can share their intellectual and cultural beliefs. Communication with the help of computers is increasing at a rapid speed. Securing this communication is of prime importance to maintain user privacy and data confidentiality. Anonymous communication systems can help us to prevent from eavesdropping and other attacks. Anonymous communication based on Onion Routing helps us to build a system that not only secures the data using multiple layers encryption but also by hiding the true sender and receiver of the data. Though there are many alternative solutions, Onion routing provides the efficient way of protection, which we have implemented.

Keywords
Onion Routing, Anonymous Communication System, AES Algorithm, File Transfer Protocol, Encryption, Decryption.

1. INTRODUCTION
Onion routing is the technique in which the information is exchanged between sender and the receiver anonymously via a number of intermediate routers known as onion routers.

Instead of establishing a minimum distance route, a random path between the sender and receiver with random number of intermediate nodes i.e. the onion routers is used for data transfer. Onion routing technique also secures the communication using multiple layers encryption. Every node has knowledge about only is previous and next router. In this way the router has no idea about the sender and receiver of the data. Also every node is assigned a key before the communication starts which is used to decrypt the outermost layer of encryption and then passes it on to the next node. Thus only the last node can access the contents of the data packet [5].

The Figure 1 explains onion routing in a more concise way.

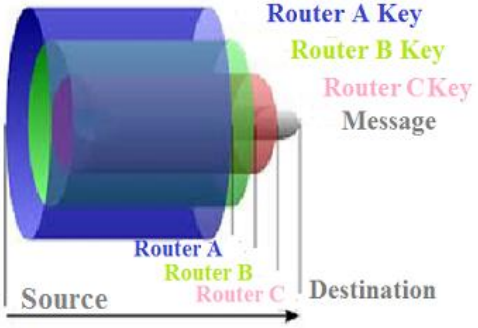

Figure 1: Basis of Onion Routing

2. CURRENT ANONYMITY SYSTEM
There are several communication systems present that provide anonymous communication. The different anonymity systems are Mix Networks, Low-Latency communication and Data publishing. The former has high latency, message oriented and can be in either one-way or two-ways. Few examples of this type are MixMaster, MixMinion, etc. The Low-Latency anonymity system include TOR(The Onion Router),JAP, Anonymous proxies and so on [4]. The latter type comprises of FreeNet, and is different from most other peer-to-peer applications, both in how users interact with it and in the security it offers. Freenet separates the underlying network structure & protocol from how users communicate with network. The contents on Freenet can be accessed in various ways and the simplest of them is using FProxy.

FProxy allows users to browse free sites. For most of configuration & node management tasks, web interface is generally used. Freenet provides the opennet and daknet, two different levels of security [6].

3. PROPOSED SYSTEM
It follows three-tier architecture with,

1. Application: it consists of Onion Routing application which is to be installed on every node.
2. Server: it comprises of web server, encryption keys, maintain and update information of online nodes, generate paths and choose a random path.
3. Data tier: it consists table of online nodes and encryption keys.

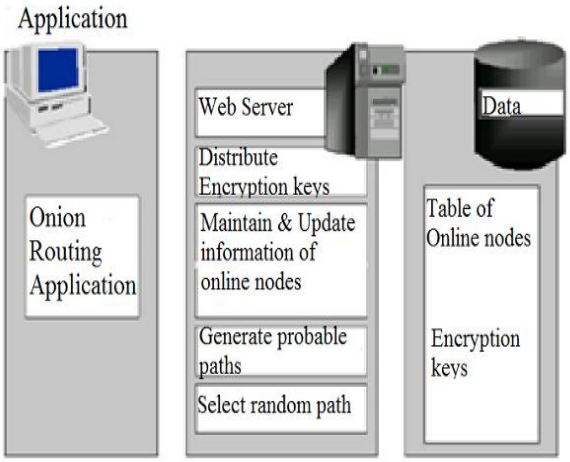

Figure 2: Conceptual Design

The Figure 3 explains the flow of the anonymity system process. Let us consider a scenario where the user wants to send a file to another user in Local Area Network (LAN). Initially the user runs the application and selects the file or message to be sent. The application creates onion (encrypting each layer with public key of router in the path) and forwards it to next Onion Router. This router decrypts the onion with it's private key and send it to subsequent routers in the path. The process continues until it reaches the destination, where it decrypts the final layer of encryption and obtains the message or final data.

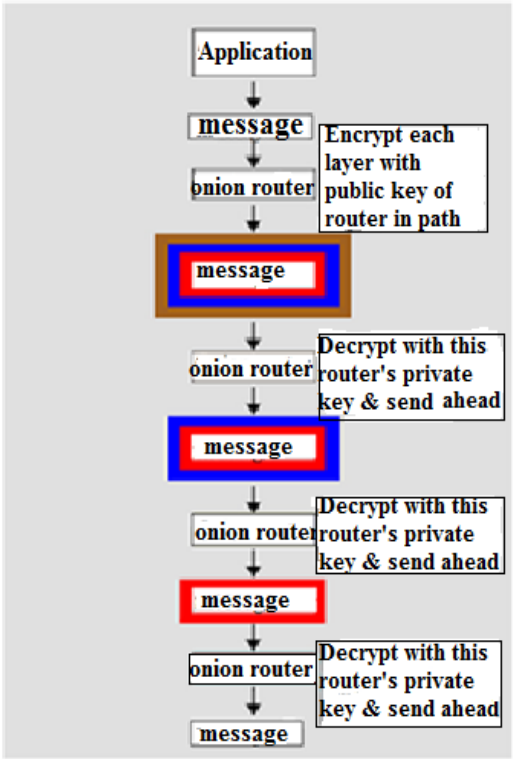

Figure 3: Flow-Chart

4. IMPLEMENTATION

Our anonymity system comprises of Onion Routers and a Server.

4.1 Working

The sender suppose node(A) selects the receiver of the data from the list of online nodes suppose node(B). The server then generates a random path ($P_{(1)}$, $P_{(2)}$, ..., $P_{(n)}$) between nodes A and B and sends it to node A. Then the sender i.e. node A creates the onion using the keys of the intermediate nodes and forwards it to the next node.

The next node $P_{(1)}$ decrypts the outer most layer of encryption with its key and gets $I[P_{(2)}]$ i.e. the IP address of the next node in the path and forwards the data packet to it.

The power of Onion routing is its recursive nature in the structure which reflects its recursive nature in the encryption decryption mechanism. In the case of structural recursion, the message contained in the outermost onion is also an onion. In the case of decryption, when a node $P_{(j)}$ receives the data packet it decrypts it with key $k_{(j)}$ and gets the IP address of the next node $I[P_{(j+1)}]$ and forwards the data packet to the next node. At the next node the same operations take place and the when the data reaches the destination node(B), it decrypts the data with $P_{(B)}$ and gets the original data sent by node(A) [1].

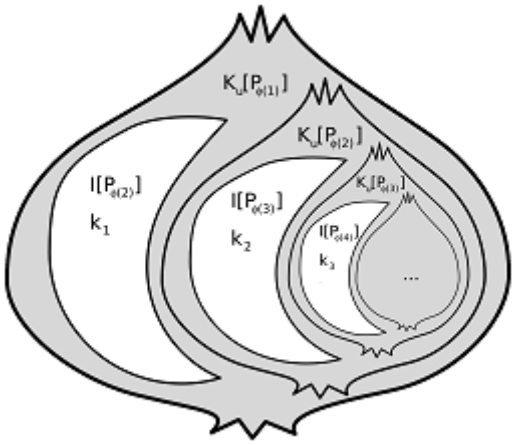

Figure 4: Onion layers: the message for each node's onion is the onion for the next node

4.2 Encryption and Decryption

Encryption is the process of converting the plain text data (or simply plain text) to something meaningless, which hides the plain text (or cipher text). While Decryption is the reverse process of encryption, i.e. it converts the cipher text to plain text. [7]. Various techniques can be used for this process such as RSA, Hash algorithm, MD5, DES and AES. We have used AES algorithm.

4.3 AES Algorithm

AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes). It uses same key to encrypt and decrypt. The cipher consists of N-rounds which depend on key length.

1. Substitute Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key

While the final round contains only three rounds, except Mix Columns.

For decryption process, the first N-1 rounds consists of the following transformations as follows:

1. Inverse Shift Rows
2. Inverse Substitute Bytes
3. Inverse mix Columns
4. Add Round key

While the final round contains only three rounds, except Inverse Mix Columns.

Figure 5 shows Encryption and decryption in AES.

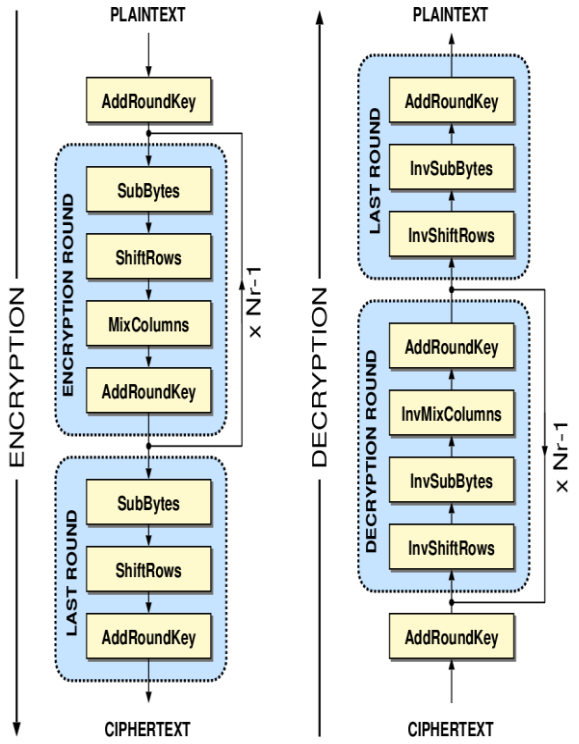

Figure 5 Encryption & Decryption in AES

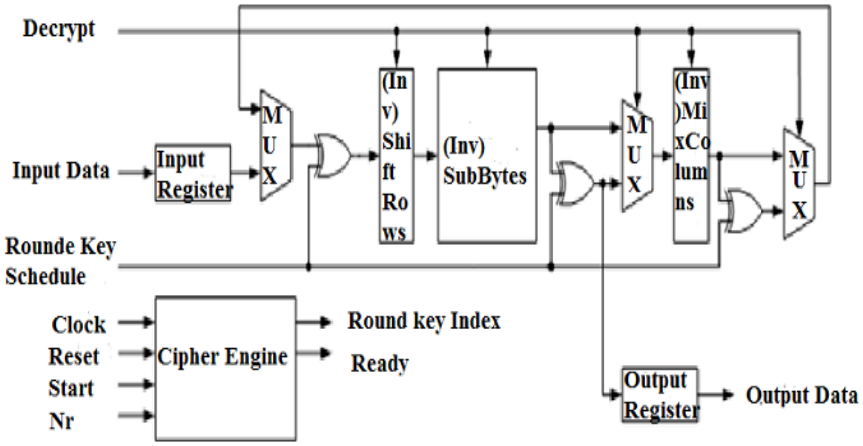

Figure 6: AES Block Diagram

4.4 Results

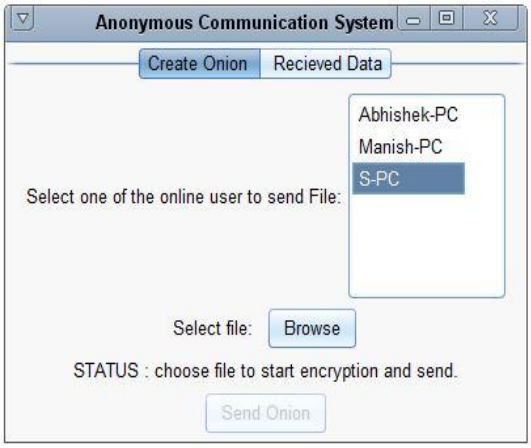

Figure 7: UI for online nodes

The Figure 7 list out the online users and allows the sender to select any online user to send the file.

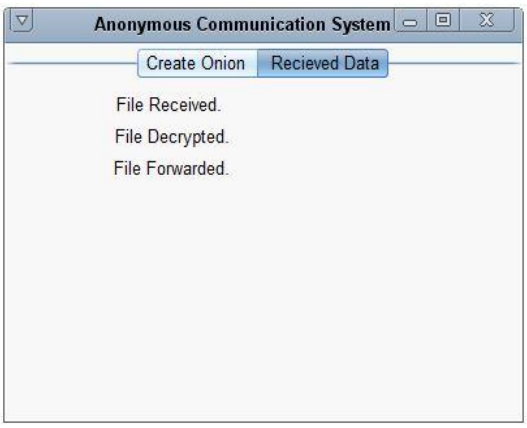

Figure 8: Status of file at intermediate node

The Figure 8 depicts that the file is received and decrypted at the intermediate node and further the file is forwarded to the next node.

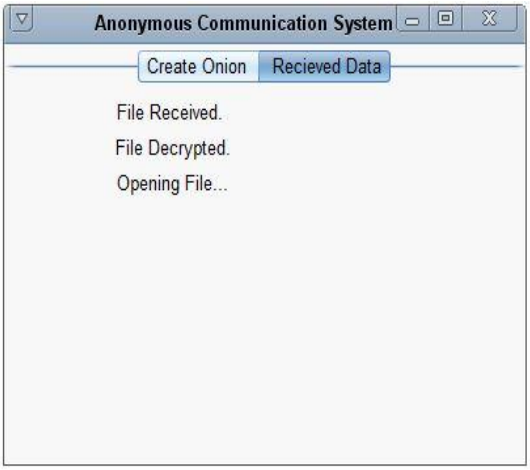

Figure 9: At destination Node

The Fig.9 shows that the file is received and decrypted at the destination node and it is in opening process.

5. CONCLUSION

Just like many other technologies, onion routing can be used for both positive and negative purposes. Criminals can evade identification in some cases using Onion Routing but this just can't be a reason for completely condemning onion routing. Anonymity is placed at the application layer. The users who are benefitting from onion routing right now are a pretty good reason for onion routing to continue. While it attracts it share of attackers, it continues to be the best tool for anonymity and free information access on the internet. It will be around for some time to come. To be effective, Onion Routing must be widely used.

6. FUTURE SCOPE

In the future, the application can be scaled to work over the internet to provide anonymity in communication. This will also require the system to choose an anonymous path considering time efficiency since the number of nodes will be large. Besides, a hybrid encryption and decryption algorithm should be developed to make the data more secure.

7. ACKNOWLEDGMENTS

We take this opportunity to thank **Dr. Mrs Nupur Giri**, Head of Department of Computer Engineering for making requisite facilities available for us.

8. REFERENCES

[1] Hooks, M., & Miles, J. (2006), "*Onion Routing and Online Anonymity"*, Duke University, Computer Science, Durham.

[2] "Onion Routing." *Wikipedia*. Wikimedia Foundation, n.d. Web. 26 June 2015. <https://en.wikipedia.org/wiki/Onion_routing>.

[3] Reed, Michael G., Paul F. Syverson, and David M. Goldschlag. Onion Routing Network for Securely Moving Data through Communication Networks. Patent US 6266704 B1. 03 Feb. 2015.

[4] "Joan Feigenbaum." *Joan Feigenbaum*. N.p., n.d. Web. 26 June 2015. <http://www.cs.yale.edu/homes/jf/>.

[5] Kumar, A., Sharma, A., Gupta, C., & Pathak, D. (2012). *Onion Routing*. IIT, Computer Science and Engineering, Kanpur.

[6] "Freenet." *Wikipedia*. Wikimedia Foundation, n.d. Web. 26 June 2015. <https://en.wikipedia.org/wiki/Freenet>.

[7] "Data Encryption and Decryption." *(Windows)*. N.p., n.d. Web. 26 June 2015. <https://msdn.microsoft.com/en-us/library/windows/desktop/aa381939(v=vs.85).aspx>.

[8] Goldschlag, D. M., Reed, M. G., & Syverson, P. F. (1996). Hiding Information routing.

[9] M. Backes, I. Goldberg,A. Kate, & E. Mohammadi (2012) 'Provably Secure and Practical Onion Routing', *Computer Security Foundations Symposium (CSF)*, (1940-1434), pp. 369 – 385.

[10] Paul Syverson () *Onion Routing*, Available at: *http://www.onion-router.net/* (Accessed: September 2014).

[11] ANIKET KATE, GREG M. ZAVERUCHA, and IAN GOLDBERG (2010) 'Pairing-Based Onion Routing with Improved Forward Secrecy', *ACM Transactions on Information and System Security*,, 13(), pp.