International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-410 PAGE NO: 2786-2790

PRIVACY AWARE SECURED COMMUNICATION BY SERVING WEB EXPLOITING EMAIL TUNNELS

R.G.Krishna Subhaa[#1], Dr.T.Velumani[*2]

[#]*Student, M.Sc Computer Science,*
Rathinam College of Arts and Science, Coimbatore,
Tamil Nadu, India-641021. subhasenthil@gmail.com

[*]Assistant Professor, Department of Computer Science,
Rathinam College of Arts and Science, Coimbatore,
Tamil Nadu, India-641021. velumani.cs@rathinam.in

Abstract: Open communications over the Internet pose serious threats to countries with repressive regimes, leading them to develop and deploy censorship mechanisms within their networks. Unfortunately, existing censorship circumvention systems do not provide high availability guarantees to their users, as censors can easily identify, hence disrupt, the traffic belonging to these systems using today's advanced censorship technologies., we propose serving the Email Tunnels, a highly available censorship-resistant infrastructure. It works by encapsulating a censored user's traffic inside email messages that are carried over public email services like Gmail and Yahoo Mail. We implement a tunneled sever that can used to reduce communication overhead among the web mail server. We propose a technique that will implement a secured data sharing via two mail account for a single user which can be used for different purposes i.e. alien mail and domestic mail. Both are secured in different ways of communication. That is mainly created to reduce the communication delay. By passing email via our tunneled server data traffic will be reduced. Even we can send the emails to blocked destinations. With the help of alien mail server the data transactions won't be leaked out even with the censorship circumvention because the data will be encrypted using efficient triple DES algorithm. Likewise the censor will not be able to identify tunneled messages from their recipient fields in domestic mail. Also, the use of steganography/encryption to embed tunneled data renders DPI (deep packet inspection) infeasible.

Keywords - Email Tunnels, Mail server, Tunneled Server, Deep Packet Inspection.

1. RELATED WORK

Our goal is to assist the project in developing a strategy to deal with any risk. For this a look at the possible risks is to be carried out, how to monitor them and how to manage the risk. For software development to avoid any risk both the developer and client have to work together. The software is to be free of any defects or errors, but it is hard or at times almost impossible to develop a system that is free of any defects.

Drawbacks:

1. Lack of security
2. Single security scheme for all transactions
3. Open Censorship circumvention analysis
4. High bandwidth consumption.

II. PROPOSED SYSTEM:

In this project, design and implement SWEET, a censorship circumvention system that provides high availability by leveraging the openness of email communications. A SWEET client, confined by a censoring ISP, tunnels its network traffic inside a series of email messages that are exchanged between herself and an email server operated by SWEET's server that includes alien mail and domestic mail. The SWEET server acts as an Internet proxy by proxying the encapsulated traffic to the requested blocked destinations.. However, a malicious third party will not be able to identify these emails since they are *proxied* by the AlienMail server running outside the censoring area. In simpler words, they only observe that the client is exchanging encrypted messages with the Alien Mail server but they can't

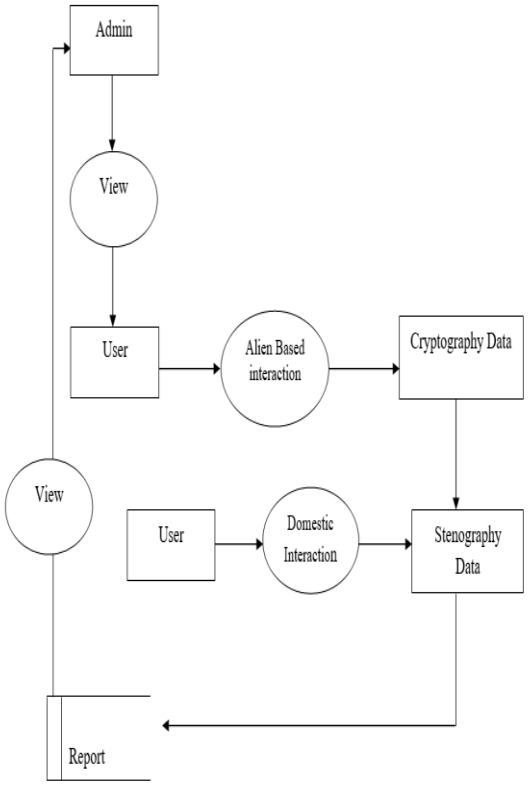
International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-410 PAGE NO: 2786-2790

access the content. In the case of Domestic Mail, the SWEET server uses a secondary *secret* email account, which is only shared with that particular client, for exchanging SWEET emails. Here we applying steganography for security purpose.

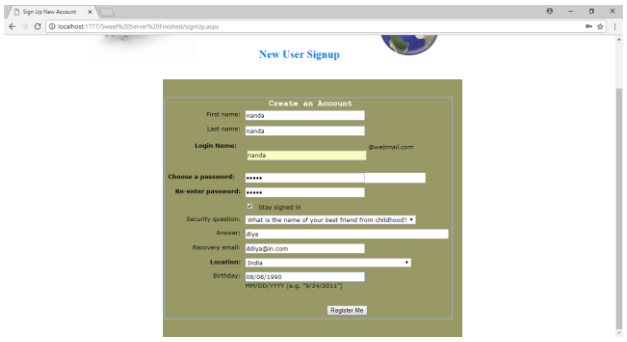
Advantages:

- Advanced security implementation with RSA and stegnography
- Transaction based security implementation
- Secured server transactions.
- Implementation of tunneled server will reduce the communication delay in web mail server.
- Consumption of network bandwidth is low.

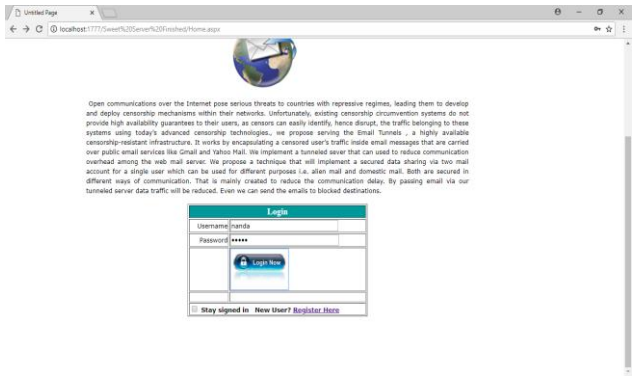
III. PROPOSED DIAGRAM

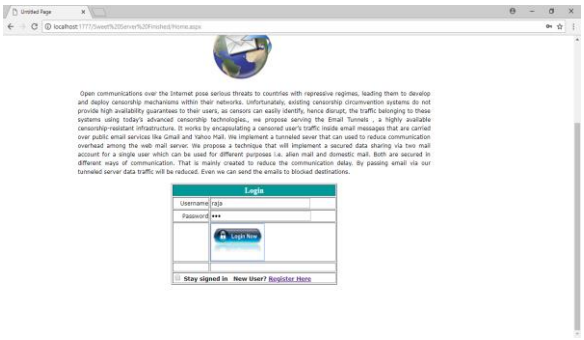


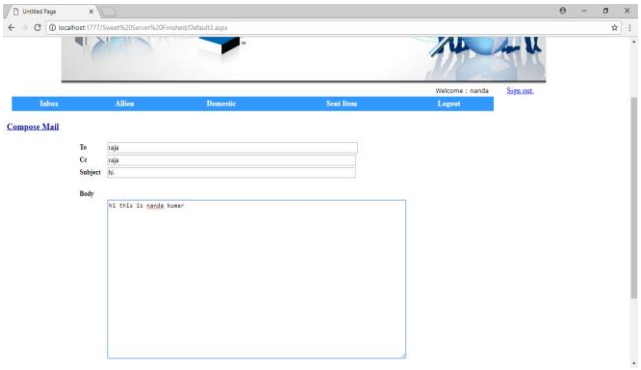
IV. OUTPUT SCREENS

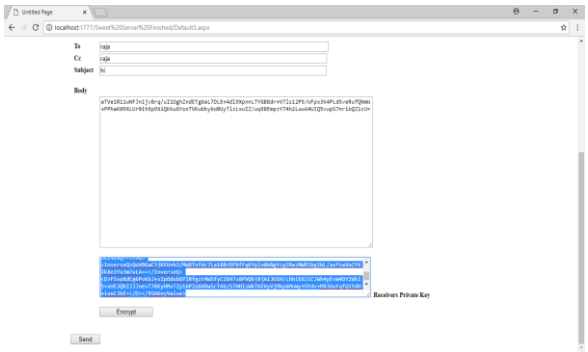


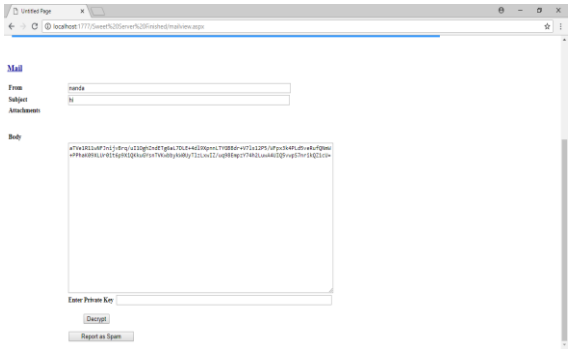
International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-410 PAGE NO: 2786-2790



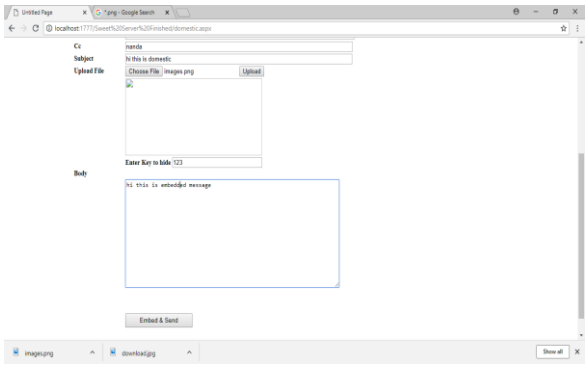


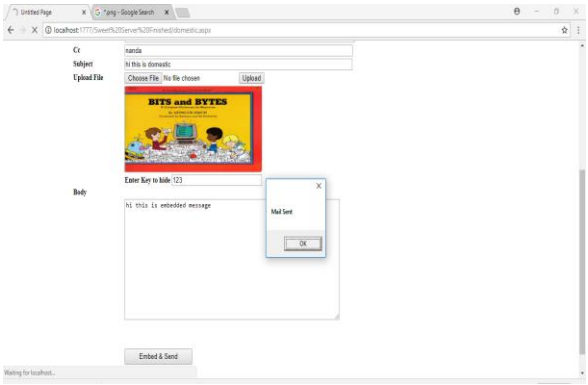


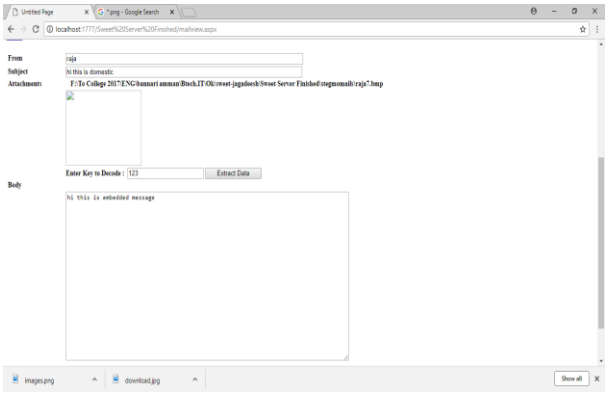


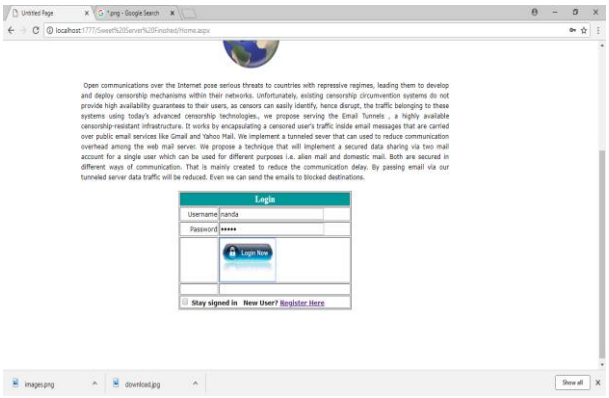


International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-410 PAGE NO: 2786-2790









V. CONCLUSION

This project is designed in order reduce the burden of maintaining bulk of records of the user and secured data. Inserting, retrieving and updating the patient details of are easy when it is compared to the offline and storing. Maintaining the project is also easy which can is easily understandable. Maintaining the details in the database is manageable. The generation of reports are computerized and quick easier then when done offline. Appropriate messages are displayed to assist to user whenever necessary. Input screens are simple and easy to understand. This project is consistent and useful one. This application has been developed to meet almost all the requirements of the user.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-410 PAGE NO: 2786-2790

REFERENCES

[1] J. Boyan. The Anonymizer: Protecting User Privacy on the Web. ComputerMediated Communication Magazine, 4(9), Sept. 1997.
[2] S. Burnett, N. Feamster, and S. Vempala. Chipping Away at Censorship Firewalls with User-Generated Content. In USENIX Security Symposium, pages 463–468. USENIX Association, 2010.
[3] C. Callanan, H. Dries-Ziekenheiner, A. Escudero-Pascual, and R. Guerra. Leaping Over the Firewall: A Review of Censorship Circumvention Tools, Mar. 2010.
[4] J. Chen, D. Hutchful, W. Thies, and L. Subramanian. Analyzing and accelerating web access in a school in peri-urban india. In WWW (Companion Volume), 2011.
[5] Clarke, T. W. Hong, S. G. Miller, O. Sandberg, and B. Wiley. Protecting Free Expression Online with Freenet. IEEE Internet Computing, 6(1):40–49, 2002.
[6] I. Cooper and J. Dilley. Known HTTP Proxy/Caching Problems. Internet RFC 3143, June 2001.
[7] R. Dingledine and N. Mathewson. Design of a blocking-resistant anonymity system. Technical report, The Tor Project, Nov. 2006.
[8] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. In M. Blaze, editor, USENIX Security Symposium, Berkeley, CA, USA, 2004. USENIX Association.