



An Approach to Virtual Learning on the LAN Based System

1.Namrata Lonare:

namratalonare2218@gmail.com

2.Manjusha Nannawar:

manjunannaware179@gmail.com

3.Pallavi uware:

pallaviuware2812@gmail.com

department of computer technology ,Mata Mahakali polytechnic,warora

Abstract—

Over the past 20 years, computer networks have introduced unprecedented opportunities for language learners to access and publish texts and multimedia materials and to communicate in new ways within and beyond the classroom. Whereas computer-assisted language learning (CALL) refers broadly to a wide range of applications (e.g., tutorials, drills, simulations, instructional games, tests etc.), network-based Virtual Drawing (NBVD) refers specifically to the pedagogical use of computers connected in either local or global networks, allowing one-to-one, one-to-many, many-to-many communication. In addition to this high security are provided for secured data transmission.

*Index Terms—*Cryptography; VOIP; Encryption;Steganography.

INTRODUCTION

A. Overview

NBVD research explores what happens when learners are brought together with texts, media, and other speakers of the language in computer-mediated contexts of interaction. NBVD arose at the confluence of both technological and educational change. In the 1980s and 1990s, networking technologies and infrastructure developed with dramatic rapidity in many industrialized countries, making low-co connections possible[3]. At the same time, educational theory and practice were increasingly influenced by social constructivism, which emphasized the social and cultural construction of knowledge, the importance of collaboration among individuals and groups, and learner- and problem-based approach to pedagogy. A virtual private network (VPN) allows the provisioning of private network services for an organization or organizations over a public or shared infrastructure such as the Internet or service provider backbone network. The shared service provider backbone network is known as the VPN backbone and is used to transport traffic for multiple VPNs, as well as possibly non-VPN traffic.

Data security is one of the most important issues for computer forensic experts. The confidential information in corporate, government offices needs to be kept secured from unauthorized users. Experts take necessary steps to keep data safe and secured from unintended users. Steganography is an art of hiding confidential information in some cover medium file [1]. It can be used to hide secret message in digital multimedia files which can be retrieved later by intended users. This technique can be used for secret communication and confidential information sharing via internet medium. This method of secret message passing is seen to be misused in offices by leaking important company documents though some cover medium files [1]. Encryption techniques along with steganography can provide high level of data security.

B. Encryption

Papers presented in ICRRTET Conference can be accessed from

<http://edupediapublications.org/journals/index.php/IJR/issue/archive>



In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption doesn't prevent hacking but it reduces the likelihood that the hacker will be able to read the data that is encrypted. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm that usually requires a secret decryption key that adversaries do not have access to.

C. Difference between Steganography And Cryptography

The goal of steganography is to hide the presence of message in carrier file or hide the fact that some communication is taking place. On the other hand, goal of cryptography is to protect data from unintended users. It involves process of making message or communication so

obscure that it cannot be understood by unintended users. Mostly people get confused between these two data protection techniques. Steganography is an alternative method used instead of encryption. If steganography and encryption techniques both are used together for data protection, the combination can provide a high level of security from data hackers. In steganography, while dealing with images, the bits are used and the changes made to least significant bits in an image can go unnoticed by the human eye. If the presence of message in file is not detected then there is no chance of any leakage of information. The message reaches safely and secretly to its destination. The message can be decrypted only if it is identified. So it has an advantage over the encryption process [5]. In encryption process, no doubt how complex algorithms are used to encrypt the message and message is transmitted to intended user.

D. Objective

In the virtual network computing (VNC) system, server machines supply not only applications and data but also an entire desktop environment that can be accessed from any LAN-connected machine using a simple software VNC. In contrast to many recent applications, which have focused on giving users access to resources located anywhere in the organization from their home computing environments, VNC provides access to home computing environments from anywhere. VNC thus provides mobile computing without requiring the user to carry any device whatsoever. In addition, VNC allows a single desktop to be accessed from several places simultaneously, thus supporting application. As per the project we have shown the chatting between server and clients as well as the secure file transfer between clients through server by using the DES (Data Encryption Standard). The DES algorithm is used for the private chatting between two clients for transferring of confidential data in the form of files and virtual drawing.

II. RELATED WORK

Two general trends characterize the bulk of current research on NBVD. The first emphasizes SLA theory and interactionist models of learning. Data analysis typically consists of quantitative counts of the occurrence of morphological, lexical, and syntactical features in online discourse [3]. The second trend, described by Kern and Warschauer (2000) in the introduction to their key collection of research articles on NBVD, is informed by sociocultural and sociocognitive theories and draws on a mixture of quantitative, qualitative ethnographic, and discourse analytic methods [2]. At issue here is not only quantifying language development, but also understanding how learners interpret and construct meaning online across culturally situated contexts. Although the primary research emphasis of each trend differs, the studies

typically share a focus on discourse written by post-secondary foreign language learners in asynchronous and synchronous environments. Although computer networks have been used for interpersonal communication since the 1960s, it was not until the 1980s that they began to serve language teaching. One of the first pedagogical uses of local area networks was to teach

Papers presented in ICRRTET Conference can be accessed from

<http://edupediapublications.org/journals/index.php/IJR/issue/archive>



writing to deaf students via synchronous conferencing at Gallaudet University. The University of Texas at Austin was another early adopter institution where synchronous conferencing was incorporated into English literature and writing courses as well as foreign language teaching (in Portuguese, German, and French)[4]. These early studies (for reviews, see Ortega, 1997, and Warschauer, 1997) pointed to a number of potential benefits of synchronous conferencing compared with face-to-face class discussions:

1. Increased and more democratically distributed student participation.
2. More time to develop and refine comments—possibly leading to greater precision and sophistication of expression.
3. Encouragement of a collaborative spirit among students.
4. Enhanced motivation for language practice and, in particular, greater involvement of students who rarely participated in oral discussions.
5. Reduction of anxiety related to oral communication in a foreign language.
6. Positive effects on students' writing ability and perhaps speaking ability as well.

The Virtual Networking Computing (VNC) system is a thin client system. Like all such systems, it reduces the amount of state maintained at the user's terminal. VNC viewers are exceedingly thin because they store no unrecoverable state at the endpoint. This contrasts with systems like X Windows, and allows arbitrary disconnection and reconnection of the client with no effect on the session at the server. Since the client can reconnect at a different location—even on the other side of the planet—VNC achieves mobile computing without requiring the user to carry computing hardware. Of course, VNC is not the only thin-client system. Others include those built around the Citrix ICA protocol (for example, Citrix's Winframe and Insignia Solutions' Ntrigue), SCO's Tarantella, Graphon's RapidX, and Microsoft's Windows-based Terminal Server (previously code-named Hydra). The problem with all of these systems except Microsoft's is that, unlike X, they use proprietary protocols, so reliable information about them is difficult to obtain. Citrix's ICA protocol is a popular mechanism for remote interaction with PCs, but it appears to be closely tied to the Microsoft Windows GUI, so it may not be an ideal general purpose remote display protocol. Microsoft has developed its own protocol, T.Share, based on the ITU T.120 protocol.



III. METHODOLOGY

A. STEPS FOR PROJECT

Network base virtual drawing and data sharing basically comprise one server and many clients.

- 1) First create server in java using java.net package having ServerSocket class with specific port number.
- 2) Then create client using Socket class.
- 3) Connect server from client by specifying address of server and port number on which server is running
- 4) Design user interface for client and server.
- 5) On each button we will call ActionListener interface to listen specific action of client and server.
- 6) Communicate between client and server by text message, file transfer and virtual drawing.
- 7) Text message from client will first transfer into byte format and then transfer to server or other client and same vice versa.
- 8) Virtual drawing from server will be converted into pixel and then transfer to client at runtime such that drawing will be shown at runtime to client.

B. DES Algorithm

DES relies upon the encryption techniques of confusion and diffusion. Confusion is accomplished through substitution. Specially chosen sections of data are substituted for corresponding sections from the original data. The choice of the substituted data is based upon the key and the original plaintext. Diffusion is accomplished through permutation. The data is permuted by rearranging the order of the various sections. These permutations, like the substitutions, are based upon the key and the original plaintext. The substitutions and permutations specified by the DES algorithm. Chosen sections of the key and the data are manipulated mathematically and then used as the input to a look-up table. In DES these tables are called the S-boxes and the P-boxes, for the substitution tables and the permutation tables, respectively.

IV. IMPLEMENTATION DETAILS

In creating this prototype server, we'll be using nothing more than the basic packages built into every Java implementation. This allows us to explore server programming at the very lowest level possible in the Java language. In many cases, the best real-world solution is to use an existing framework, because it often provides useful features such as fault-tolerance, load-balancing, and seasoning. The word framework has a technical definition within the object-oriented community means a design structure that can be reused.

This is not the same as traditional code reuse, in which bits of code written for one purpose (or for no particular purpose at all) are reused for a new purpose. Rather, a framework is a reusable, overarching structure inside which you can implement your particular application. Structuring it that way would distract from the purpose of this tutorial, which is to explore basic techniques of server programming. We can create our own connection-oriented server from following steps:

Papers presented in ICRRTET Conference can be accessed from

<http://edupediapublications.org/journals/index.php/IJR/issue/archive>



The seven elements are:

- * Listener class
- * While-Accept loop
- * Per-Thread class
- * While-Read/Write loop (Server side)
- * Removing dead connections
- * Client class
- * While-Read/Write loop (Client side)

Two Major Software Components :

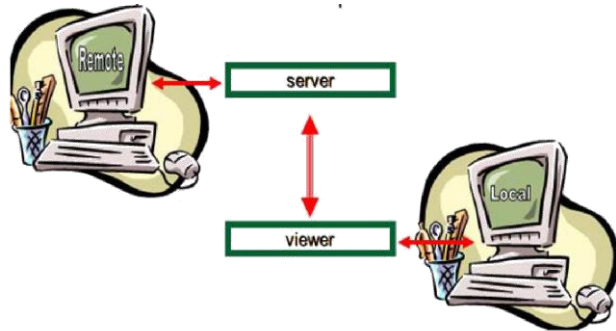


Figure 4.1 Software Component

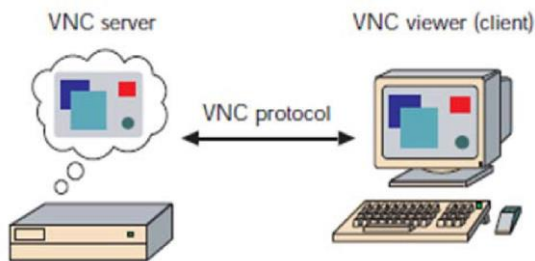


Figure 4.2 VNC Architecture

V. EXPERIMENTS AND RESULTS

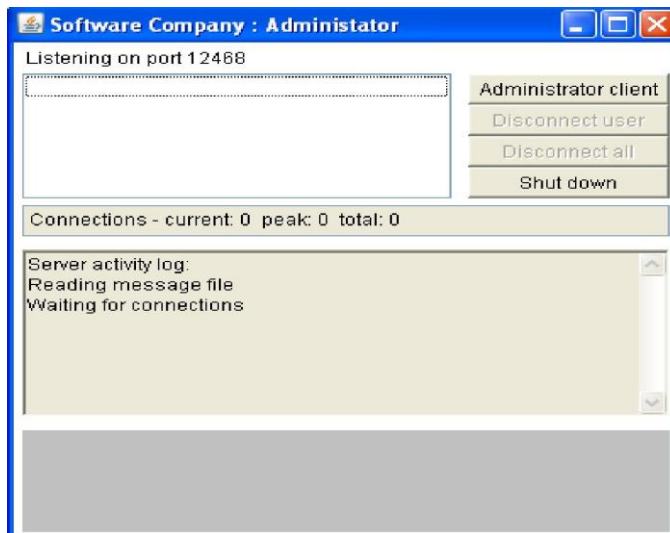


Fig 5.2 Administrator U.I

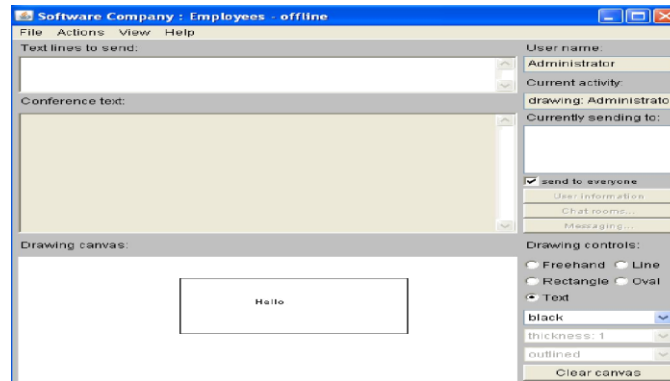


Fig 5.3 U.I. of Client with Virtual Drawing.

VI.

CONCLUSION

The accelerating diffusion of digital media and wireless networks, together with the increased naturalization of computer mediated communication, promises that NBVD will remain a critical area for teaching and research. The network itself has changed dramatically in recent years, with the rapid spread of participatory tools and sites facilitating social networking, interactive game playing, collaborativ writing and editing, and multimodal production. These tools provide opportunities for students in read, write, communicate, and construct knowledge explored. VII. FUTURE SCOPE

This technology has come to include tactile feedback. Many learning resources employ the sense of touch to involve learners. The haptic technology can benefit the children with special needs especially visually impaired and also be used to successfully teach concepts i physics and math. It allows for a more interactive learning experience which could be potentially implemented across a wide range of subjects. The other future prospects in Web based learning is new network which can offer opportunities to virtual learning environments Thus, it accelerates the interactive learning in virtual classrooms. Of course, these developments require much more organization and imaginations than simply placing text on network. Future developments in virtual learning environments may also embrace wireless and portable

devices.

REFERENCES

- [1] Jiantao Zhou, Xianming Liu, Oscar C. Au, Fellow, and Yuan Yan Tang, Fellow, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation", In: IEEE Transactions on information forensic and security, vol.9, No.1, January 2014.
- [2] Black, R.W., , 'Access and affiliation: The literacy and composition practices of English language learners in an online fanfiction community', Journal of Adolescent and Adult Literacy 49(2), 118-128, 2005.
- [3] Abrams, Z.I., 'The effect of synchronous and asynchronous CMC on oral performance in German', Modern Language Journal 87(2), 157-167, 2003.
- [4] Belz, J.A., 'Linguistic perspectives on the development of intercultural competence in tele collaboration', Language Learning and Technology 7(2), 68-99, 2003.
- [5] Monica Adriana Dagadit, Emil Ioan Slusanschi ,Razvan Dobre, "Data Hiding Using Steganography", In: IEEE 12th International Symposium on Parallel and



Distributed Computing, 2013.

[6] Asjad Amin, Haseeb Ahmad Qureshi, Muhammad Junaid, “Run Length Encoding Scheme with Introduction of Bit Stuffing for efficient Data Compression”, International Conference for internet Technology and Secured Transactions, 2011.

[7] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, “A commutative digital image watermarking and encryption method in the tree structured Haar transform domain,” Signal Pro-cessing: Image Commun., vol. 26, no. 1, pp. 1–12, 2011.

[8] X. Zhang, “Lossy compression and iterative reconstruction for en- crypted image,” IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[9] Kodituwakku.S.R, Amarasinghe.U.S., “ Comparison of Lossless Data Compression Algorithms for Text Data”, Indian Journal of Computer Science and Engineering, vol.1,No.(4), pp. 416 – 425,2009.

[10]L. C.-Chiang, W. H.-Chu, T. C.-Shyong, C. Y.-Ping,

”Adaptive lossless steganographic scheme with centralized difference expansion”, Pattern Recognition 41, pp. 2097–106, 2008.

[11] Blake, R., ‘Bimodal CMC: The glue of language learning at a distance’, CALICO Journal 22(3),497–511, 2005.

[12] T. Richardson et al., “Teleporting in an X Window System Environment,” *IEEE Personal Comm* .,No. 3, pp. 6-12. Also available as ORL Technical Report 94.4, ORL, Cambridge CB2 1QA, England, 1994.

[13] Furstenberg, G., Levet, S., English, K., and Maillat, K., ‘Giving a virtual voice to the silent language of culture: The CULTURA project’, Language Learning and Technology 5(1), 55–102, 2001.

[14] William Stallings , “Cryptography and Network Security Principles and Practice”, 90-121, 2011.

[15] O. P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi, “Performance Analysis of Data Encryption Algorithms”.