Secure Transmission with Matrix Encryption and Data Compression Mechanism

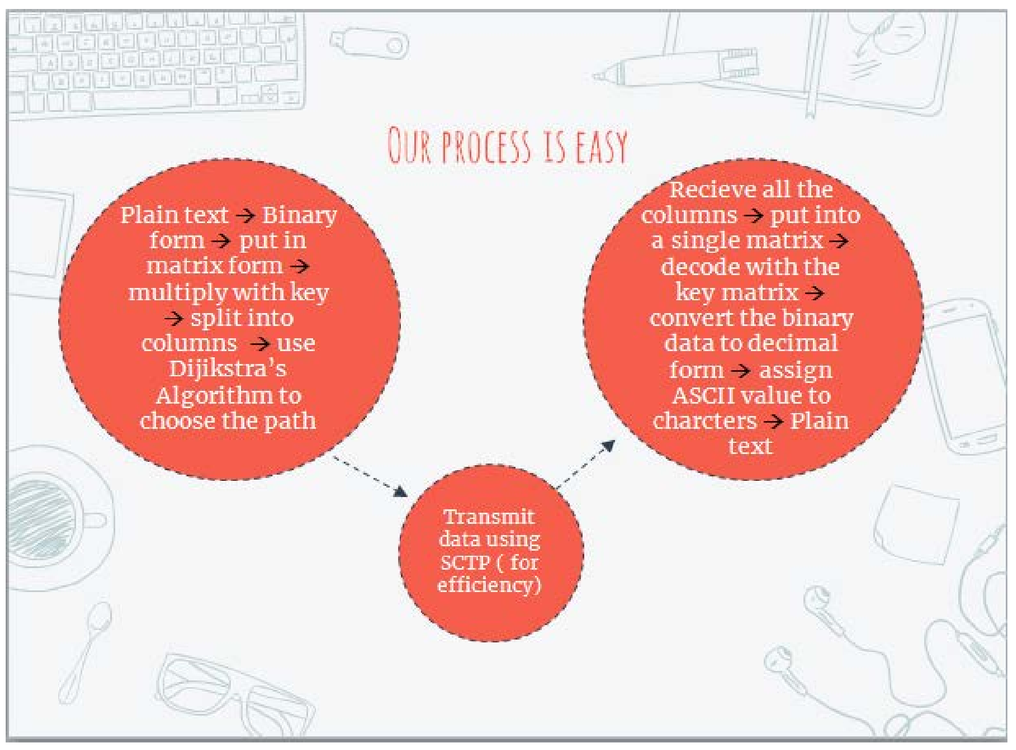
Abul Hasan Fazulullah, Kartavi Patel, Dipesh Patel, Purva Vansia
Poster Advisor: Dr. Abdel-shakour A. Abuzneid
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract:

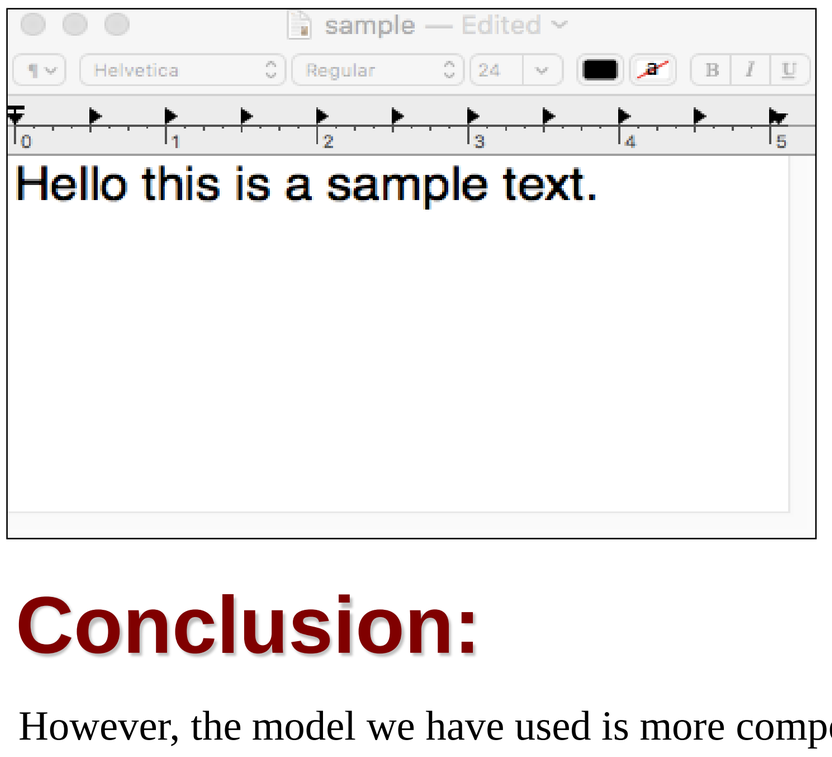
With emerging technology and support for 4G and 5G network, considering Internet and Intranet, the bandwidth is not a big of a problem as it was before. The main concern now is the implementation of security and how efficiently we can send the data to recipients. We have come up with an awesome concept that takes confidentiality and availability as mainstream. The idea in simple words is like our concept in addition to Dijkstra's algorithm running on SCTP will provide an excellent secure transmission of data over the network. The focus of our research is on how to handle the data in a different way so that we can reduce the amount of space needed for storage and helps to reduce the time and space complexity. This goal will again be helpful when there is a huge junk of data to be sent over the internet in a split of a second. The intent of using SCTP (Stream Control Transmission Protocol) is that it is more reliable and has high throughput both in proactive and reactive manner.

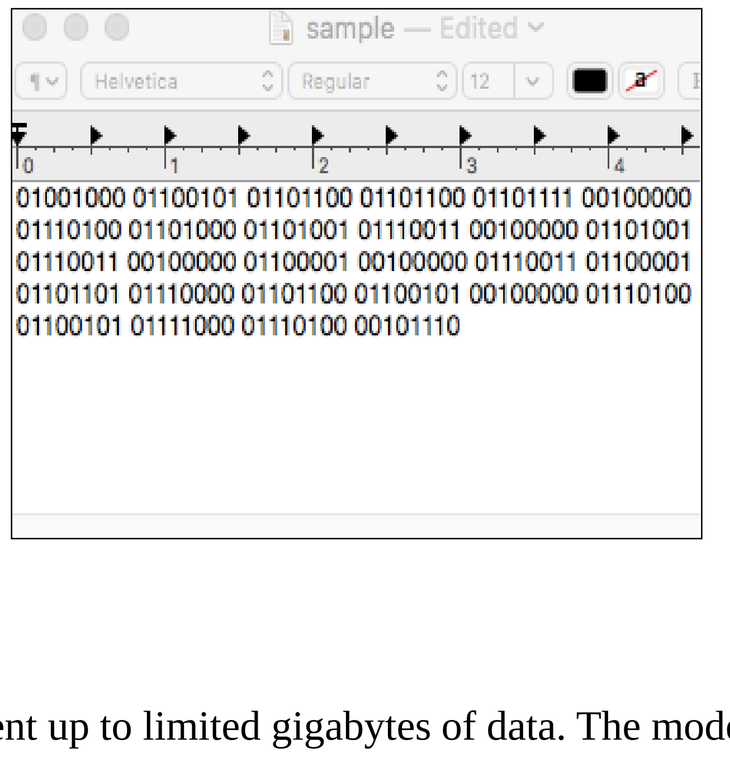
Work Flow:

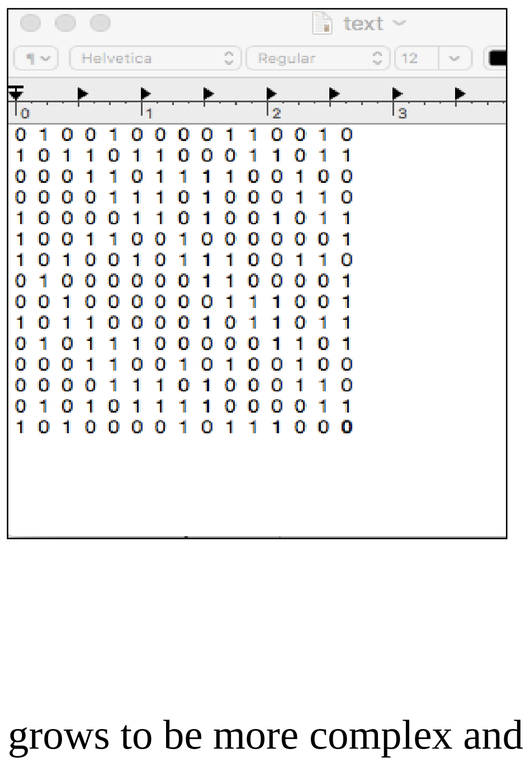
1. The data file is created.
2. All the characters in the data file are converted into integers.
3. These integers are then converted into binary numbers.
4. These binary characters are then arranged in a matrix form.
5. This binary matrix is multiplied by another random matrix, which is an encryption key.
6. Now, this newly generated matrix is split into columns by multiplying the whole matrix with each column of the identity matrix.
7. Now, each obtained columns are saved as separate bin files.
8. Each file takes up different paths and reaches the destination node.
9. At the destination end, all the bin files are combined into a single file using the tag numbers.
10. Once a single file is generated, the same encryption key is used here to decrypt the data.
11. Now the reverse process of the operation that happened at the sender end happens at the receiver end to obtain the original data.



PROTOCOLS / METHODOLOGY	PROACTIVE	REACTIVE
	Throughput in %	
SCTP	38.6%[a.]	52%
TCP	22%	17%







Conclusion:

However, the model we have used is more competent up to limited gigabytes of data. The model grows to be more complex and takes time when it deals with data in tetra bytes. This prototype works efficiently with a matrix size of 1024*1024. Increasing the size of the matrix more than this will eventually slow down the process of compression and encryption. If the complexity does not matter then this concept is the best go for highly secured transmission.