Abstract—Present scenario suggests many audio files are needed to be transmitted over internet for various important purposes. Earlier cryptographic schemes for secret sharing lead to high computational complexity during both secret sharing and secret reconstruction phase. Today, various cryptographic methods for secret sharing are there to protect secret data but everything depends on the protection of encryption key. But, most of the available cryptographic methods leads to chance of key compromise and single point failure. To overcome this problem shared cryptography scheme becomes best solution. In shared cryptography scheme, a shared secret is a small piece of secret data, known only to the parties involved in a secure communication channel. A new model is proposed for computationally secure online secret sharing, which allow dynamically changing the secret and adding participants, without having to redistribute new shares secretly to the current participants. The security of the scheme is based on the intractability of factoring. This can be achieved by using simple graphical masking method, which include two phases: Sharing data and encryption of each share. Share generation is performed by simple ANDing and reconstruction can be done by performing simple ORing the qualified set of qualified shares. Not only the generated shares are compressed but also get encrypted and each encrypted share contains partial secret information, that leads to added protection to the secret data and reduced bandwidth requirement for transmission over internet. In addition to these we are achieving efficient recovery of original secret audio data.

Keywords—Shared Cryptography Scheme, Secret Sharing, Masking, Encryption, Masking, Audio Sharing, Security, Compression.

I. INTRODUCTION

Since the early introduction of Internet, it used most of the time for military purpose and later personal usage. The confidential messages intended for a limited audience are transmitted using internet. How can these messages be transmitted secretly over Internet so that no unauthorized person gets knowledge of the detailed content of messages? And how can one guarantee that a message arrives in the authorized person hands exactly as it was transmitted?

These questions arose since it has been proven many times that data on the internet is not safe, data can be easily tampered. For this reason we use the different cryptographic techniques. Traditionally, there are two ways to answer such questions. One can cover the very existence of a message, perhaps by writing with invisible ink; or try to transmit the message via a authorized person. A totally different approach is to encrypt a message. In this case one does not cloak its existence. There is a satisfying appropriateness to cryptology’s role in the birth of modern electronic computing. The arrival of the Information Age has revealed an urgent need for cryptography in the emerging private sector. Today, vast amounts of sensitive information such as health and legal records, financial transactions, credit ratings and the like are routinely exchanged between computers via public communication services [8]. Society turns to the cryptographer for help in ensuring the privacy, authenticity and integrity of such sensitive information.

Cryptography stands for the art of protecting information or data by transforming it (encrypting it) into an unreadable format, which is called cipher text or encrypted text. Only those who possess a secret key can decipher (or decrypt) the message into plain text or decrypted text. Cryptography is used to protect e-mail’s, credit card or debit card information, corporate data and many more. Cryptography systems can be broadly classified into symmetric-key cryptography that use a single key that both the sender and recipient have, public-key cryptography that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. Steganography, where message is encrypted in picture or images and videos. This is basically a variant of threshold cryptography, which deals with sharing sensitive secret among a group of n users so that only when a sufficient number k (k ≤ n) of them come together, the secret can be reconstructed. Well known secret sharing schemes (SSS) in the literature include Shamir[1] based on polynomial interpolation, Blakley[2] based on hyper plane geometry and Asmuth-Bloom[3] based on Chinese Remainder theorem.
In all of above secret sharing schemes, each share hold the complete secret information in encrypted or ciphered form. We have suggested a different concept, where simple graphical masking (ANDing) technique is used for shared generation and all the shares contain partial secret information and reconstruction is done by simply ORing the predefined minimal set of shares.

Secret sharing is an very important and widely studied tool in cryptography and distributed computation. Informally, a secret sharing scheme is a protocol in which a sender distributes a secret among a set of participants such that only specific subsets of them, defined by the access structure, can reconstruct or recover the secret at a later time. Most of research in the area of secret sharing has focused on the size of the shares. Although the size of the shares is important because the shares have to be transmitted and stored secretly in the database, this is not the only information the participants must know to reconstruct the secret. Additional knowledge needed includes, for example, the identity of the participants and the detailed description of the protocol, including the access structure. These parameters are publicly known, but at the same time it is important that they are authentic, i.e. that no malicious or unknown participant has changed these descriptions [9].

The original motivation for audio secret sharing are: (1) To safeguard cryptographic keys from loss or to be get stolen, it is desirable to create backup copies of key’s, although these copies are themselves a security risk. Secret sharing scheme addresses this issue by allowing enhanced reliability without increased security risk, (2) They also facilitate distributed trust or shared control for critical activities by requiring cooperation by t out of n users for access to a critical action and, (3) The idea of secret sharing is to start with a secret, and divide it into pieces called as shares which are distributed amongst users or participants, such that the pooled shares of specific subsets of users allow reconstruction or recovery of the original secret. This may be considered as a key distribution technique, facilitating one-time key establishment, wherein the recovered key is pre-defined (static), and in the basic case, same for all groups.

Today, In all of available secret sharing schemes, each share hold the whole secret information in encrypted or ciphered form. We have suggested a different concept, where simple graphical masking (ANDing) technique is used for shared generation and all the shares contain partial secret information and reconstruction is done by simply ORing the predefined minimal set of shares.

The success of the scheme depends upon the mask generation, a step wise algorithm is suggested for such mask design for any (k, n) scheme where n numbers of masks are designed to generate n different shares and any k shares on ORing reconstruct the original secret. Here we have further proposed an unique compression technique on the shares as a solution towards bandwidth requirement.

This paper is organized in following manner. In Section II, Detailed Literature review is given. Section III, describes Problem definition based on the literature survey. Section IV, describes the detailed architecture of proposed system. In Section V, one can find the detailed working of proposed system i.e. Secret sharing phase and secret reconstruction or data recovery phase. Finally Section VI summarizes the conclusion of the paper.

II. LITERATURE REVIEW

Secret sharing schemes were discovered independently by Shamir and Blakley. The motivation for secret sharing is secure key management. The initial applications of secret sharing were safeguarding cryptographic keys and providing shared access to strategic resources. In some situations, there is usually one secret key that provides access to many important files. If such a key is lost (for example, the person who knows the key becomes unavailable, or the computer which stores the key is destroyed), then all the important files become inaccessible. The basic idea in secret sharing is to divide the secret key into pieces and distribute the pieces to different persons in a group so that certain subsets of the group can get together to recover the key. As a very simple example, consider the following scheme that includes a group of n people. Each person is given a share Si, which is a random bit string of a fixed specified length [10]. The secret is the bit string

\[ S = S_1 \oplus S_2 \oplus \cdots \oplus S_n \]

A general secret sharing scheme specifies the minimal sets of users who are able to recover the secret by sharing their secret information. Note that all shares are needed to recover the secret. A variant of threshold cryptography, which deals with sharing sensitive secret among a group of n users so that only when a sufficient number k (k ≤ n) of them come together, the secret can be reconstructed. Well known secret sharing schemes (SSS) in the literature include Shamir[1] based on polynomial interpolation, Blakley[2] based on hyper plane geometry and Asmuth-Bloom[3] based on Chinese Remainder theorem.
Threshold Secret sharing scheme proposed by Shamir [1] based on a polynomial of degree (k-1) to any set of k points that lie on the polynomial. The method is to create a polynomial of degree (k-1) as follows:

\[ f(x) = d_0 + d_1x^1 + d_2x^2 + \ldots + d_{k-1}x^{k-1} \pmod{p} \]

Where, \(d_0\) is the secret and \(p\) is a prime number and the remaining coefficients picked at random. Next find \(n\) points on the curve and give one to each of the participants. When at least \(k\) out of the \(n\) participants reveal their points, there is sufficient information to fit an (k-1)th degree polynomial and then the secret value \(d_0\) can be easily obtained by using Lagrange Interpolation.

Blakley geometric threshold secret sharing scheme [2] used geometry to solve the secret sharing problem. The secret message is a point in a k-dimensional space and \(n\) shares are affine hyperplanes that intersect in this point. The set solution \(x = (x_1, x_2, x_3, \ldots, x_k)\) to an equation \(a_{11}x_1 + a_{21}x_2 + \ldots + a_{k1}x_k = b\) forms an affine hyperplane [11]. The secret, the intersection point, is obtained by finding the intersection of any \(k\) of these planes. Asmuth-Bloom [3] proposed a threshold secret sharing scheme in which reduction modulo operation is used for share generation and the secret is recovered by essentially solving the system of congruence using Chinese Remainder Theorem (CRT). Although the threshold secret sharing schemes based on the Chinese Remainder Theorem are not perfect, by choosing carefully the parameters, these schemes can lead to a reasonable factor: Security/No. of Shares.

In 1998 Desmedt, S. Hou and J. Quisquater [4] proposed an audio cryptography scheme. It is a secret sharing scheme that high (low) volume represents the secret bit “1” ("0") embedded into an audio signal, and the decoder for this audio cryptography scheme is the “ears” of listener. Due to constructive and destructive interference of sound waves, one can hear the volume changing. However, the authors also generalized the 2-out-of-2 to a 2-out-of-n scheme. However, the 2-out-of-n scheme needs different pieces of sounds as the cover sounds, where the word “cover” represents the sound used to embed or hide the shared secret message. More cover sounds will cause the human hearing system to overload, and one may not interpret the volume changing correctly. High cover sounds will be more difficult for the human hearing system to hear the secret.

Lin et al. [5] in 2003 proposed a new audio secret sharing scheme which uses the technique of time division with only one cover sound.

The effect of this is that when enough shares are played simultaneously the human auditory system can detect changes in the sound volume. Destructive interference results in low volume, while constructive interference results in high volume. The changes in the sound volume reveal the secret binary message, in the sense that the high volume segment corresponds to 1 and the low volume segment corresponds to 0 [12]. A new ASSS which in addition to all above properties is ideal. Ideal in the sense that the size of each share is equal to the size of the secret. ASSS is a secret sharing scheme in which the shares and/or the secret are is an audio file(s). We are interested in ASSS due to audio applications. It is likely that the secret is not a bit string or visual and we deal with audio secrets. In these cases, it could be desired to reconstruct the audio secret without any computation. In a perfect ASSS with an audio secret the following conditions hold: i) Every authorized subset could recognize the audio secret by pooling their shares together. ii) Every unauthorized subset could not reach a non-random audio file by pooling their shares together (i.e. the mutual information between the secret file and the obtained file by an unauthorized subset should be zero).

Mohammad Ehdiaie et al. [6] have proposed a novel audio secret sharing scheme. They had implemented (k, n) audio cryptography scheme in that n shares are created for encryption and k shares are used for decryption. Audio share files are thus created and audio secret is obtained only by playing k shares, simultaneously, each of this is amplified by a certain coefficient. Therefore, the secret is reconstructed without any computation. They had implemented this scheme using MATLAB. Actually in this scheme they had divided audio file into small intervals to the ith interval as Ai and finding the vector array. Then finally multiplying the every value of Ai, with some constant value c.

Ultra Secured and Authentic Key Distribution Protocol using a Novel Secret Sharing Technique [7] proposed that protection of sensitive data is an important issue, precisely during transmission over internet. Efficient cryptographic methods are there to protect data but everything depends on the protection of the encryption key. Threshold cryptography enables the construction of reliable and robust key management system which can reconstruct the key even in the destroy of some shares and on the contrary the key cannot be reconstructed unless a predefined set of shares are been accumulated.
Above all secret sharing schemes are regarded as a Perfect Secret Sharing (PSS) scheme because coalition of (k-1) shares doesn’t expose any information about the secret. A shortcoming of above secret sharing schemes is the need to reveal the secret shares during the reconstruction phase. The system would be more secure if the subject function can be computed without revealing the secret shares or reconstructing the secret back. This is known as function sharing problem where the function’s computation is distributed according to underlying SSS such that distributed parts of computation are carried out by individual user and then the partial results can be combined to yield the final result without disclosing the individual secrets. Various function sharing protocols are been proposed [13], [14], [15], [16], [17], [18], [19] mostly based on Shamir’s secret sharing as the underlying scheme. Some work [20] is also available on Blakley’s secret sharing scheme, and Asmuth-Bloom scheme [21] as well.

III. PROBLEM DEFINITION

The literature survey elaborates the fact that there are number of deficiencies as well as scope for improvement in audio secret sharing. Developing a more secure audio secret sharing scheme is challenging task, but for that we need to remove following drawbacks detected in earlier available secret sharing schemes:

1. Those lead to high computational complexity during both sharing and reconstructing.
2. Compromise of encryption key
3. Single point failure
4. Secret data hacking
5. High consumption of network bandwidth

As mentioned earlier, the computational complexity in our scheme is extremely low as it applies simple graphical masking method, done by simple ANDing for share generation and reconstruction can be done by simple ORing the qualified set of shares.

This makes it effective for addressing energy saving distributed environment where battery driven low end processors are used and security is also a major challenge.

In this work, an attempt is made to develop a audio secret sharing scheme which reduces bandwidth requirement for transmission of secret data. Most of times highly secure information which might be an audio file, image or text file is saved with the help of key by only which the user can get premises to access the data, but if information is precisely important then user never take chance that key get lost key that’s why he usually replicate the key and make many copies of same key and store them in different location. But this would increase the risk of the key being stolen or compromised.

In our scheme, we have proposed to divide any information into multiple shares. These different shares are to be transmitted via multiple disjoint paths between the pair of communicating nodes. We have proposed to send these shares at different point of time, if possible. At the receiving end the original information is reconstructed by combining the received shares.

IV. ARCHITECTURE OF PROPOSED SYSTEM

In this project our aim is to build a Internet based message transmitting application implementing novel secret sharing scheme which employs simple graphical masking method using simple ANDing for share generation and reconstruction can be done by simple ORing the predefined minimal number of shares.

Even though this working is not related to traditional client-server model, role of server here in this merely to hold data in secure manner. As in the system architecture diagram Client side operations consists Sender and receiver side operations but since both of operations require common graphics user interface. Therefore they are combined in the system architecture diagram.
The Proposed System architecture shown above basically consist of three major blocks: (1) Client side Operations, (2) Internet, and (3) Server Side Operations.

A. Client Side Operations

The client can be both either Sender or Receiver, in any case sender or receiver both uses GUI to access application according to their requirements. As block diagram shown in Figure 2 applicable only for sender side operations.

1. Each block shows its function and working at sender side.
2. Working from top to bottom from Masking to final step compression.
3. Multiple arrows facing outwards denotes data from sender side sent via various channels to add secure transmission throughout.
As block diagram shown in Figure 3 application for receiver side operations as its working, almost opposite to sender side, as in order to regenerate original message received message goes through these operations and multiple incoming arrows denotes incoming data from multiple channels.

Figure 3: Receiver Side Operations (Receiver Console)

B. Internet

Internet block from the system architecture only suggest all data transmits through in wide area network to reach destination and hence all the operations are performed to transmit data safe throughout journey using multiple channels.

C. Server Side Operations

The Server in our case multiple servers simulates multiple channels, as data arrived from clients stored randomly on servers, making it difficult to track flow. Also server serve as repository for all records, history, transmission and access to old data.

V. WORKING OF THE PROPOSED SYSTEM

The working of our proposed system mainly divided into two phases: (1) Secret Sharing Phase, and (2) Secret Data Reconstruction or Recovery Phase. In each of these two phases, we have to generate a mask which used to perform logically ANDing at sharing phase similarly it used for logically ORing at reconstruction phase. While generating mask we should consider that each mask will have a fixed number of zeros present similarly each and every bit position will represent 1 for k number of time from mask set.

To get desired such set of mask we need to follow mask generation algorithm which will select only those number from n sized binary number whose binary form is holding k-1 number of zeros and (n-k+1) numbers of 1’s and arrange them in the form of a matrix. Obvious dimension of the matrix will be nCk-1 × n. where n represent number of share and k represent (threshold) i.e number of share by ORing which we will get original message but not less than that [7]. Now convert those selected number into binary form and generate one matrix and finally take transform of resulted matrix your bunch of mask is ready.

A. Secret Sharing Phase

Sharing phase consists of major operations concerning to securing data, ANDing with pre generated mask, compress each share, encrypt it and send it with recipient’s address, we will also try to implement multiple routes for each share so that intruder cannot interfere or each share with random path will confuse hackers.

B. Secret Data Reconstruction or Recovery Phase

At receiving end we have to consider that we will get any number of shares, then first operation which we will perform, we will separate share part and header part then distinguish each and every part of share like encryption key, share number, total number. then we will get encryption key and generate a digest of 16 byte and again we will generate a mask at receiving end which is use to perform logical ORing share which we have got to get desired original secret audio.

This is our proposed system to transmit secured message, in further implementation we will also provide secured database so that user can browse through history or access previously received or sent data and keep records. Here we have further proposed an unique compression technique on the shares as a solution towards bandwidth requirement.

The process mentioned above can be applied to any binary format file for example Wav, BMP etc. In our case Wav file is converted in to Byte array, which later converted in binary form most probably 8 bit format or 16 bit in some cases, ANDed with Masks, encrypted, compressed and processed reversed on the receiving side. We will improve on User Interface by developing a ‘web app’ so that application will be accessible through anywhere and platform independent.
VI. CONCLUSION

Thus, with the implementation of Secret Sharing algorithm based on Novel Scheme or Perfect Sharing Scheme Audio file (Wav. Or any binary file) can be broken into shares, compressed, encrypted and sent over to recipient with this level of security scheme, the original data can be retrieve even if some of shares get lost during the transmission since data is scattered over each share and can be regenerated at receiver side. On plus side even if intruder gets access to a single or more number of shares (less than threshold) it is helpless to regenerate original message. We presented an efficient secret sharing approach with minimal computational overhead. In our future effort we will try to implement cover medium method based on Steganography, in this concept of cryptography the shares are sent in cover medium which may be image, audio or video which will make each share a meaningful file and difficult for attacker to understand actual data behind it.

REFERENCES