HIGHLY SECURE CRYPTOGRAPHY ALGORITHM METHOD TO SAFEGUARD AUDIOS AND VISUALS

Janaki Raman Palaniappan

Software Engineer, USA

ABSTRACT

Internet hacking has become common now a days and is increasing day by day. It is a high time to safeguard our data. There are several cryptographic methods and algorithms that are evolved and already exist. How about additional protection makes us stress free? In this paper, I present a unique design of cryptographic algorithm which is specifically designed for Auditory cryptography and visual cryptography to make the encryption and decryption technique stronger. The purpose is to make it very difficult to decode the file when an unauthorized user accesses the data. This algorithm is a combination of multiple techniques such as Ant Algorithm, Logical Gates Technique, Dual authorization PINs, Indexed Arrays. Combination of these techniques makes the algorithm unique and strong to secure the data. This research was implemented on audio files, images and video files. The study of the result shows effective way of masking the data as it is hard to decode without PINs. Also, performance of the algorithm is efficient during encryption and decryption process.

KEYWORDS

Auditory Cryptography, Visual Cryptography, Ant Algorithm, Logic Gates, Indexed Arrays

1. INTRODUCTION

Cryptography is often referred to as secret writing to maintain the confidentiality. This means the data is transformed into non-readable content, to make it a readable content one need to convert it using the secret keys. Only authorized user will be able to read the data. On a day today basis we share our details in the form of data content, audios, images, videos and so on through various internet medias for various reasons like job search, apply license, book tickets and so on. Organizations reads the data, sell the data from these files to develop a strategy for their business needs and growth. A sample fact, we would have given a phone number in a website for a purpose. Few days later we get a call from anonymous numbers for various promotions. This may be a data leak or data sold.

Our major responsibility is to protect the data before sharing them to prevent brute force and other attacks. Efficient way is to encrypt the file in our local device. We must remember to transform messages in a way that are hard to decipher. Hence using the strong and efficient algorithm is always a priority. This paper discusses about a unique algorithm that is a combination of multiple different techniques which results in very efficient as well as difficult to decode the data. Dual Authorization PINs plays an important role between the user and the algorithm, Ant Algorithm helps in encryption and decryption process to be faster as path details are maintained, Logical Gates Technique is used for masking the PINs as an additional security, Indexed Arrays helps monitoring the stages of the encryption and decryption. These techniques combined evolved as a complex algorithm that prevents Bruce force attacks and other internet attacks.

2. CRYPTOGRAPHY

Cryptography term is derived from the Greek word Kryptos which means hidden. Cryptography is the technique to mask the information through use of codes and allows only authorized user to view the content.

Cryptography is widely used due to great security.

Cryptography is broadly divided into 2 categories,
Single Key or Secret Key – In this method, Same single key must be used by both sender and receiver. Sender can use any key of the choice to encrypt the content. Receiver must use the same secret key that was used by sender to decrypt the content. It is also known as Symmetric Key cryptography.

Public Key – This method uses a pair of keys to Encrypt and Decrypt the data. A public key is associated with the creator while encryption whereas the private key is associated with the receiver to decrypt the content. It is also known as Asymmetric key cryptography.

2.1. Auditory Cryptography

Auditory Cryptography is a terminology used to secure the audio files. The algorithm will be applied to audio files to protect it safely. After encryption the audio file will be inaudible state meaning the file is masked. Authorized used can decrypt the file and it will be converted to audible state. Once the file is audible state then user can hear it.

2.2. Visual Cryptography

Visual Cryptography is a technical term that is used when the images and videos are to be encrypted and decrypted. Encryption takes place when the visual files are converted into a non-readable format. An authorized user who has secret pins is only allowed to decrypt the data. As soon as the file is decrypted, the visual appears the same.

3. ANT ALGORITHM

ANT Algorithm is based on the ANT behavior when it searches for the food. This procedure helps in optimizing the problem of finding the best path on a weighted graph. Ant lives in colonies. Ants start wander randomly in search of food. Once the ant finds the source of the food, it starts depositing the pheromone markers on the path and goes back to the colony. But it is based on the quantity of pheromone markers the other ants follow which path to choose. Ant that reaches the colony earlier could have dropped more markers on the path. The ants can smell the markers and certainly follow the markers to reach the food. When the quantity of marker is more on the path that means source of the food is short. When multiple times the path is followed has more markers and has higher probability to follow the path next time. This optimizes the path to shorter for the ants to reach the destination. This algorithm technique will be used in the cryptography algorithm for a better performance on decryption.

4. ANALYSIS AND RESEARCH OF ALGORITHM

Experiment was done on different classification of files such as Audio files, Image files and Video files. There are many algorithms exist to do the cryptography. I decided to take a different

unique approach to design an algorithm that is high effective and efficient. Also, the idea is to cipher the file at local device itself.

At the starting phase of the algorithm the user must provide the path where the file is located. Algorithm asks user to provide must DUAL PIN (x1, x2) for authentication purpose. First pin is upto 4-digit secret code and the second pin is a single digit secret code. These PINs acts as a secret key to do the cryptographic process. In this algorithm symmetric key method is followed, so these DUAL PIN must be entered correctly by receiver to decrypt the file successfully.

DUAL PINs are masked by the algorithm for an additional security. As the PINs details are carried away with the file across the internet to the receiver location, hence attacking is possible. For this reason PINs are masked to a different value internally using logical gates. Masked PINs are used for further processing across the algorithm.

Encryption is a combination of multiple techniques such as the use of DUAL PIN, Logical gates, array of bytes, Ant Algorithm and Indexed arrays on how the file has to be encrypted. This combination provides a high protection to the data. If an user wants to view the visual or hear the audio file, decoding DUAL PIN is must. Combination of DUAL PIN makes it difficult for anyone to hack it.

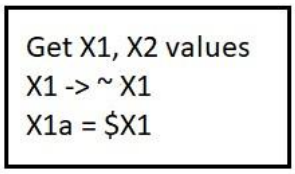


Figure 1. Representation of dual pin

The algorithm is intelligent enough to understand whether the auditory cryptography or visual cryptography takes place based on the extension of the file. The Input file is initially converted into series of array of bytes and is stored in the file itself. Next the masked first secret PIN of DUAL PIN is combined with series of array of bytes to form a cipher converted new series array of bytes and stored in the file itself. At this stage, the file has non-readable content.

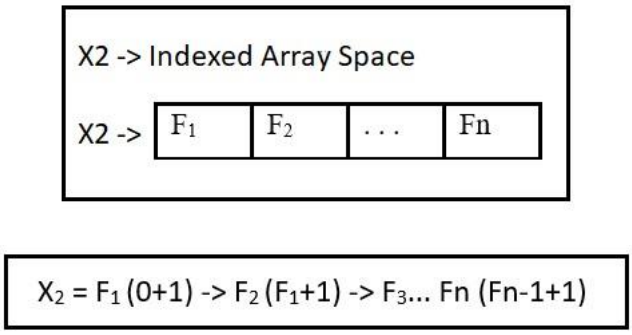
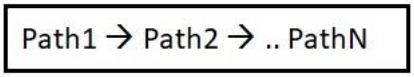


Figure 2 . Representation of Indexed Array space

Algorithm is designed in such a way based on the second pin value; the distance of the destination is determined. The Ant algorithm technique is used to decide on how long the encryption technique must travel. Second pin value decides the number of stages that it has to pass through the travel before reaching final stage of encryption. At each stage new masked first pin is generated. This masked pin are passed through Indexed Array and is used to capture the values.

Values are stored in an order the way stage encryption takes place. This Indexed array method helps us in guiding the shortest efficient path as the masked pin is never the same. Based on the number of stages, at each stage the new set of series of array of bytes is generated as it is a combination of new masked pin and the last set of series of array of bytes and will be captured in the file. At each stage the values are written to the same file. At the last stage, it contains a last of series of array of bytes and is stored in the file. Last stage is the destination, and it is where the file is completely encrypted and ready to share. This design makes the DUAL PIN stronger. This acts as a double protection and multiple encryptions technique applied to the file. The user is safe to transfer the file to someone or save in an email, etc. It is encrypted and in non-readable content.



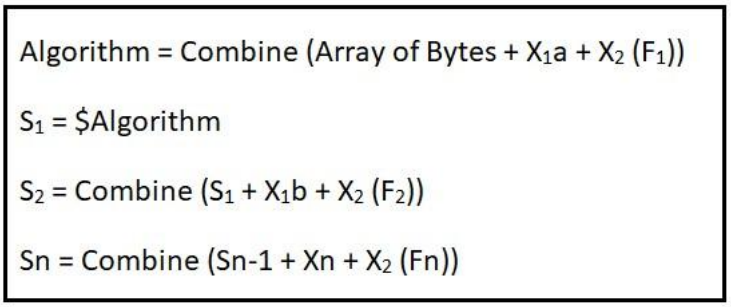


Figure 3. Depicts the Encryption

If any third party tries to read the content when the file is transferred, it would be in a stage where it is very difficult to decode. Once the file reaches the destination, user can decrypt the file to view the content. As the symmetric key method is followed here, A receiver must provide DUAL PIN to be able to decrypt the content of the file.

At the receiver end, the user has to provide the location of the file to the algorithm. Once the algorithm starts the process, it expects the user to input the DUAL PIN. As soon as the user provides the DUAL PIN, algorithm starts the decryption process of the file. Remember, here the image contains series of array of bytes as it was encrypted at final stage of encryption. When the user enters the incorrect PIN of either of a dual pin then the file gets corrupted because it starts to decrypts the file with incorrect PINs. For this reason, it is suggested to have copy of the file if the user do not remember the PIN so that user can retry the decrypt process once again with the proper file. The other option is to cross check with the sender if the PIN is correct as algorithm follows symmetric key method.

Ant algorithm plays a major role in decryption process as it helps the algorithm to follow the travel path (markers) of encryption technique that was tracked by Indexed array. Input file has the series of array of bytes which is unknown to the user. If the user tries to open the file, pop up window says unable to open file. First secret pin is again one step reverse masked to travel to the stages. The algorithm combines the series of array of bytes and first secret pin and produces a new set of series of bytes and is stored in the file. Concurrently the secret pin is captured in the new Indexed array and pointed to the encrypted Indexed array to monitor the stages (markers of the ant). Indexed Array is very important as it helps to achieve the short path for an efficient performance of the algorithm.

At each stage the Indexed array monitors and captures the value of the reverse masked first secret pin. At every stage first secret pin is reversed and is still masked. Also combining the series of arrays of bytes and reverse masked first secret pin takes place where the new set of series of array of bytes generates. This process follows at each stage where a different set of series of array of bytes being generated. Indexed array is being tracked in the reverse way to reach the destination. At the last stage, final set of decryption takes place.

$$\text{Path1} \rightarrow \text{Path2} \rightarrow .. \text{PathN}$$

$$\text{Algorithm} = \text{Combine (Encrypted file} + \text{rev}(X_1a + X_2 (F_1)))$$

$$Sn = \$\text{Algorithm}$$

$$S_2 = \text{Combine (Sn} + \text{rev}(X_1b + X_2 (F_2)))$$

$$S_1 = \text{combine (}S_2 + \text{rev}(Xn + X_2 (Fn)))$$

Figure 4. Depicts the Decryption

As the Indexed array reaches the starting point meaning the last step of the process, algorithm understands that it is last stage of decryption and further travel is not needed. At this phase, the file is completely decrypted. User will be able to view or hear the content of the file based on whether the file is audio, image or video.

The flow of the algorithm process has been picturized in the form of flow chart that gives overall picture has been shown below,

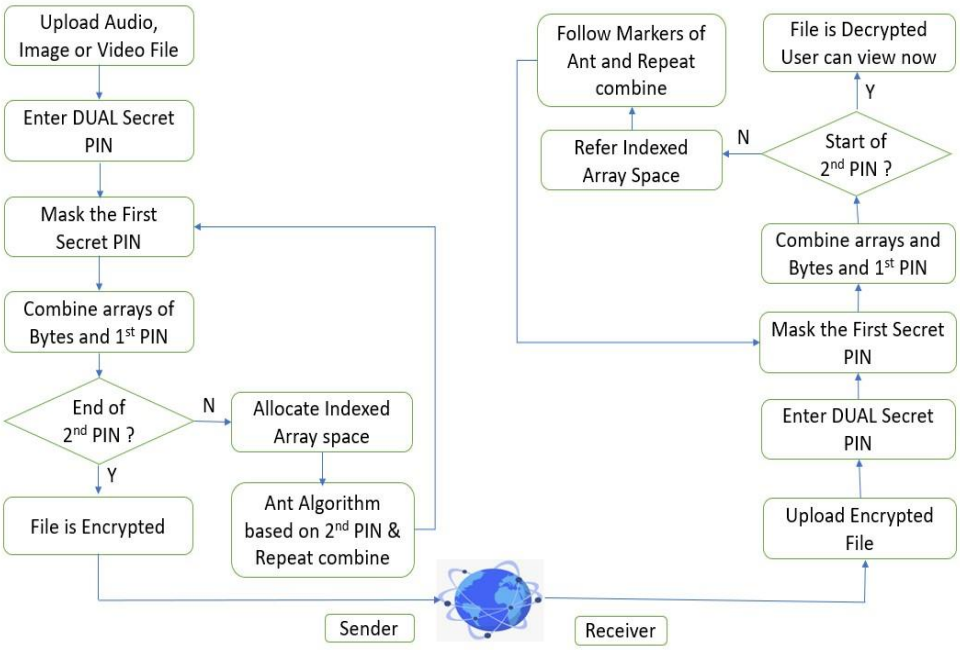


Figure 5. Flow Chart of the algorithm

4.1. Sample Results

Auditory Cryptography

ORIGINAL AUDIO FILE .AAC → ENCRYPTION ARRAYS → NON-AUDIBLE FILE → DECRYPTION ARRAYS → ORIGINAL AUDIO FILE .AAC

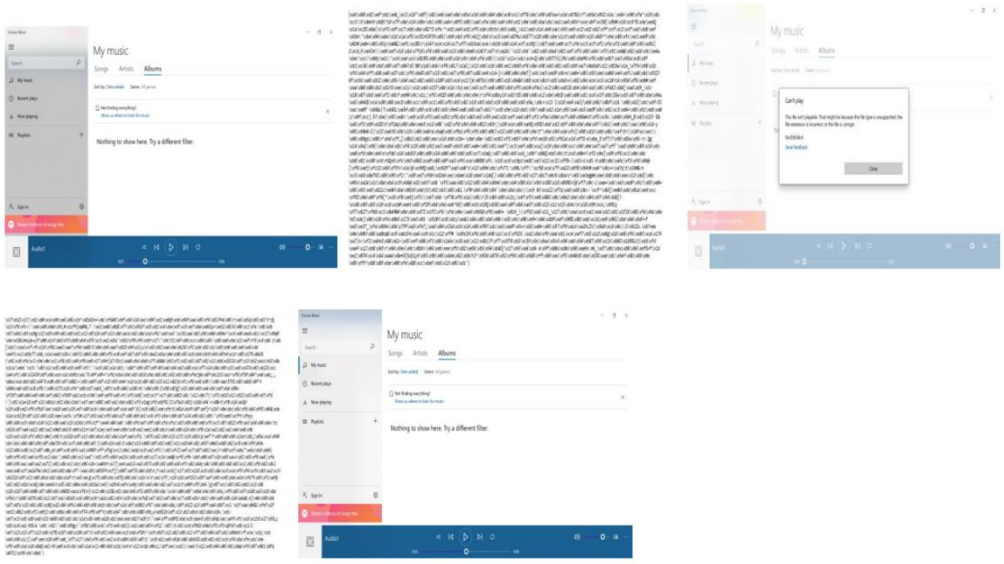


Figure 6. AAC format encrypt/decrypt output

Visual Cryptography

Image

ORIGINAL IMAGE FILE .PNG → ENCRYPTION ARRAYS → UNREADABLE FILE →DECRYPTION ARRAYS → ORIGINAL IMAGE FILE .PNG

Figure 7. PNG format encrypt/decrypt output

Video

ORIGINAL VIDEO FILE .MP4 →→ ENCRYPTION ARRAYS → NON-VIEWABLE FILE → DECRYPTION ARRAYS → ORIGINAL VIDEO FILE .MP4

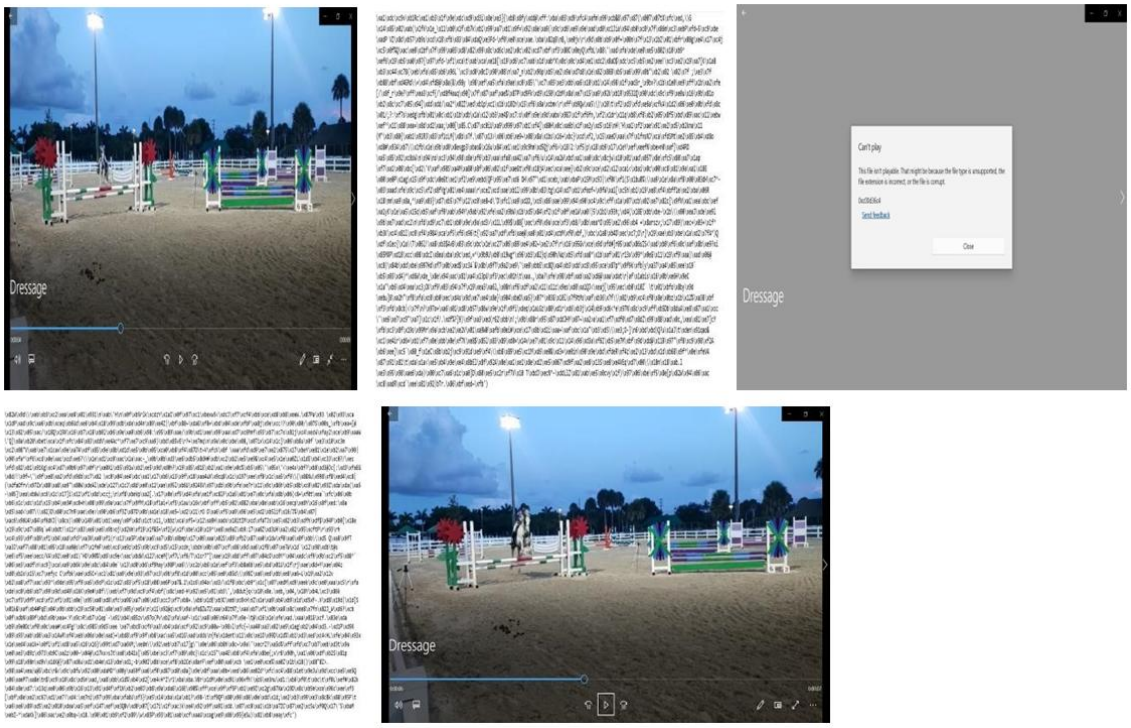


Figure 8. MP4 format encrypt/decrypt output

4.2. Tabulation Comparison

Audio/ Image/ Video File	Size of the File	Degree of 2nd PIN	Time taken to Encrypt	Time taken to Decrypt without Indexed Array	Time taken to Decrypt with Indexed Array
Audio2.mp3	2.23 MB	Low	2.65 secs	2.66 secs	2.43 secs
Audio2.mp3	2.23 MB	Medium	5.35 secs	5.23 secs	5.10 secs
Audio1.aac	78 KB	High	323 ms	461 ms	290 ms
Audio1.aac	78 KB	Low	4 ms	3 ms	3 ms
Audio1.aac	78 KB	Medium	111 ms	93 ms	90 ms
mahal.jpg	171 KB	Medium	532 ms	441 ms	400 ms
mahal.jpg	171 KB	Low	308 ms	307 ms	291 ms
PP.png	74 KB	Low	149 ms	123 ms	115 ms
PP.png	74 KB	Medium	216 ms	202 ms	192 ms
PP.png	74 KB	High	310 ms	340 ms	345 ms
Egg.jpg	4.07 MB	Low	5.1 secs	5.0 secs	5.0 secs
Egg.jpg	4.07 MB	Medium	16.8 secs	15.91 secs	13.83 secs
Egg.jpg	4.07 MB	High	26.6 secs	26.2 secs	25.1 secs
Sand.jpg	6.90 MB	Medium	56.12 secs	43.48 secs	43.40 secs
Sand.jpg	6.90 MB	High	57.26 secs	1 min 1 sec	1 min 10 secs
vid.mp4	193 KB	Low	342 ms	254 ms	220 ms
vid.mp4	193 KB	Medium	455 ms	434 ms	401 ms
vid.mp4	193 KB	High	683 ms	553 ms	490 ms
park.mp4	23 MB	Low	117 secs	108 secs	90 ms
park.mp4	23 MB	High	313 secs	248 secs	241 ms
hills.png	2.35 MB	Medium	8.17 secs	7.85 secs	7 secs
hills.png	2.35 MB	High	5.78 secs	5.68 secs	4.50 secs
Music.ogg	12 KB	Medium	2 ms	32 secs	10 ms
Music.ogg	12 KB	High	3 ms	38 secs	3 ms
Dressage.mp4	3.44 MB	Low	56.38 secs	44.26 secs	48.10 secs
Dressage.mp4	3.44 MB	Medium	7.33 secs	7.47 secs	6.01 secs
Dressage.mp4	3.44 MB	High	14.83 secs	12.12 secs	10.12 secs
Pan.png	94 KB	Low	219 ms	213 ms	200 ms
Pan.png	94 KB	Medium	316 ms	302 ms	280 ms
Pan.png	94 KB	High	401 ms	420 ms	390 secs
GC.gif	923 KB	Low	1.35 secs	1.23 secs	1.01 secs
GC.gif	923 KB	High	3.96 secs	3.48 secs	3.29 secs
Audio3.M4A	384 KB	Low	34 ms	33 ms	33 ms
Audio3.M4A	384 KB	Medium	95 ms	93 ms	90 ms
Audio3.M4A	384 KB	High	1.71 secs	1.73 secs	1.59 secs

Figure 9. Table Comparison output

4.3. Tabulation Discussion

100+ different variety of files such as audio, image and video of different formats with the different sizes have been experimented for the analysis and the part of results are given in the Figure 4.2.1 above. The experiment was done based on the size of the files, 2nd secret PIN level of degree, With and without Indexed Array space allocation where ANT algorithm based technique is implemented.

Based on the second Secret PIN entered, logic gate technique combination of array of bytes values and the inverted first secret code value happens and written them as series of bytes back into the image and it is repeated at each stage. At each stage, the indexed array is entered and monitored and same is used while decryption process for the better performance.

Two different experiment analysis have been shown in the table Figure 4.2.1. First experiment analysis was without indexed array allocation technique and the result was 80% of the scenario, time taken for the decryption was faster than the time taken for the encryption. Second experiment analysis was with indexed array allocation technique and the result was 95% of the scenario, time taken for the decryption was faster than the time taken for the encryption. This comparison result shows the effective performance when Indexed Array space allocation technique along with ANT algorithm logic was very efficient to find the origin of the encrypted file. Also, we need to remember the factor where while we do the analysis that there are several other factors that consume time like CPU, Memory, system load, etc.

5. CONCLUSION

This research reveals the effectiveness of unique method of securing the data at source device. Dual PIN secret code authentication makes the algorithm hard for any hacker to decode any type of file as combination of PINs could be a quite more numbers and incorrect code corrupt the file. Indexed Array and ANT algorithm technique helps the decryption process faster than the encryption. It monitors and captures the stages and follow the markers while reaching back the origin. The combination of multiple techniques used in this algorithm makes sure the content of the file is safe and secure thus makes the user stress free.

REFERENCES

[1] Ant algorithm for grid scheduling problem - IPP – BAS, Acad. G. Bonchev, bl.25A, by Stefka Fidanova & Mariya Durchova

[2] Crypto your Belongings by Two Pin Authentication using Ant Algorithm based Techniqueby Janaki Raman Palaniappan, Brunswick Corporation, USA - CAIML - Volume 12, Number 12, July 2022.

[3] Wayner, P. : Disappearing Cryptography, Morgan Kaufmann Publisher, 2002

[4] Encryption and Decryption Standard) for data security - Ali Mohammed Ali Argabi, Md Imran Alam - IARJSET - Vol. 6, Issue 10, October 2019

[5] Research on Various Cryptography Techniques - Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi

[6] Cryptographic Algorithm For Enhancing Data Security: A Theoretical Approach by Tushar , Aniket Sharma , Ankit Mishra - IJERT - Volume 10, Issue 03, March 2021

[7] Implementing generic security requirements in e-voting using modified stegano-cryptographic approach - Int. J. Information and Computer Security, Vol. 7, No. 1, 2015 by Olaniyi Olayemi Mikail, Omidiora Olusayo, E. Okediran, Elijah Olusayo

AUTHOR

Janaki Raman Palaniappan is a Software Engineer working in USA. He obtained his B. Tech in 2009 in Information Technology. He is currently a Researcher, Database Administrator and a Cloud Engineer. He has published in reputable Journals and Learned Conferences. His area of research is mainly on Cryptography, Information Security, Image Processing, Databases and Cloud.