International Journal of Pure and Applied Mathematics
Volume 116 No. 10 2017, 301-308
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A Modified Symmetric Key Cryptography Method for Secure Data Transmission

Dr. M. Ilayaraja[1], Dr. K.Shankar[2], Dr. G. Devika[3]
Assistant Professor[1,2,3],
School of Computing,
Kalasalingam University,
Krishnankoil, – 626126, Tamil Nadu, India.
ilayaraja.m@klu.ac.in[1], shankar.k@klu.ac.in[2], devika.g@klu.ac.in[3]

***Abstract* - Cryptography is necessary when communicating over any untrusted medium, like internet. It is possible to access and modify by unauthorized persons while transferring the data from one to another. Cryptography plays a significant role in the field of information security. Nowadays, cryptographic techniques are used to secure the data from hackers in various fields. One of the most commonly used cryptosystem is symmetric key encryption which uses single key for both encryption and decryption. In this paper, a modified Caesar cipher symmetric key encryption method developed to convert the actual message into secret information using mathematical principles. Plaintext contains alphabets with case sensitive, numbers and special characters into secret information. The proposed technique produces the ciphertext includes more number of special characters. The result of the proposed method proves that it is very difficult to identify the original message from the encrypted message.**

Index Terms - Caesar Cipher, Encryption, Decryption, Cryptography, Symmetric Key, Network Security.

I. INTRODUCTION

The word cryptography comes from the Greek words Crypto and Graphy. Crypto means Secret and Graphy means Writing [1]. Cryptography deals with creating documents that can be shared secretly over public communication channels. Cryptography is the study of creating and using encryption and decryption techniques. An encryption algorithm works with a key to transform the plaintext into ciphertext. Decryption algorithm works in the reverse order and converts the ciphertext into. Usually key is a number that is mixed with plaintext to yield ciphertext. The enciphering or encryption is a process of converting plaintext into ciphertext. deciphering or decryption is a process of retaining the plaintext from the ciphertext. In general cryptography is used to achieve authentication, confidentiality, integrity and non-repudiation to ensure reliability of data.

Cryptography is grouped into Symmetric Key and Asymmetric Key Cryptography [3]. In Symmetric key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions. The Asymmetric Key Cryptography uses different keys for both processes. The encryption key is public so that anyone can encrypt a message. However, the decryption key is private, so that only the receiver is able to decrypt the message. It is common to set up "key-pairs" within a network so that each user has a public and private key. The public key is made available to everyone so that they can send messages, but the private key is only made available to the person it belongs to[4].

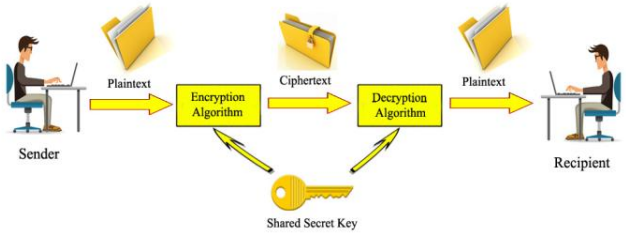

Fig. 1 Encryption/Decryption Process

Two types of ciphers are used in Symmetric Key Cryptography. They are stream cipher and block cipher. Stream ciphers encrypt the bits of information one at a time - operate on 1 bit of data at a time. Stream ciphers are faster and smaller to implement than block ciphers, however, they have an important security gap. If the same key stream is used, certain types of attacks may cause the information to be revealed. Block cipher is a symmetric cipher which encrypts information by breaking it down into blocks and encrypting data in each block. A block cipher encrypts data in fixed sized blocks [5]. In this paper, developed an efficient symmetric key encryption method to send the information secretly.

II. CAESAR CIPHER

The simplest possible substitution cipher is the Caesar cipher, reportedly used by Julius Caesar during the Gallic Wars. Each letter in the plaintext is replaced by a letter shifted a fixed number of places to the right. We regard the

alphabet as a cycle, so that the letter following Z is A. Thus, for example, the table below shows a right shift of 5 places.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

The message "Send a hundred slaves as tribute to Rome" would be enciphered as XJSI F MZSIWJI XQFAJX FX YWNGZYJ YT WTRJ. The key is simply the number of places that the letters are shifted, and the cipher is decrypted by applying the shift in the opposite direction (five places back). Some practical details make the cipher harder to read. In particular, it would be sensible to ignore the distinction between capital and lower case letters, and also to ignore the spaces between words [2]. The Caesar cipher is not difficult to break. There are only 26 possible keys, and one can try them all.

XJSI F MZSIWJI XQFAJX FX YWNGZYJ YT WTRJ

KEY								
1	WIRH	E	LYRHVIH	WPEZIW	EW	XVMFYXI	XS	VSQI
2	VHQG	D	KXQGUHG	VODYHV	DV	WULEXWH	WR	URPH
3	UGPF	C	JWPFTGF	UNCXGU	CU	VTKDWVG	VQ	TQOG
4	TFOE	B	IVOESFE	TMBWFT	BT	USJCVUF	UP	SPNF
5	SEND	A	HUNDRED	SLAVES	AS	TRIBUTE	TO	ROME
6	RDMC	Z	GTMCQDC	RKZUCR	ZR	SQHATSD	SN	RNLD
7	QCLB	Y	FSLBPCB	QJYTBQ	YQ	RPGZSRC	RM	QMKC
8	PBKA	X	ERKAOBA	PIXSAP	XP	QOFYRQB	QL	PLJB
9	OAJZ	W	DQJZNAZ	OHWRZO	WO	PNEXQPA	PK	OKIA
10	NZIY	V	CPIYMZY	NGVQYN	VN	OMDWPOZ	OJ	NJHZ
11	MYHX	U	BOHXLYX	MFUPXM	UM	NLCVONY	NI	MIGY
12	LXGW	T	ANGWKXW	LETOWL	TL	MKBUNMX	MH	LHFX
13	KWFV	S	ZMFVJWV	KDSNVK	SK	LJATMLW	LG	KGEW
14	JVEU	R	YLEUIVU	JCRMUJ	RJ	KIZSLKV	KF	JFDV
15	IUDT	Q	XKDTHUT	IBQLTI	QI	JHYRKJU	JE	IECU
16	HTCS	P	WJCSGTS	HAPKSH	PH	IGXQJIT	ID	HDBT
17	GSBR	O	VIBRFSR	GZOJRG	OG	HFWPIHS	HC	GCAS
18	FRAQ	N	UHAQERQ	FYNIQF	NF	GEVOHGR	GB	FBZR
19	EQZP	M	TGZPDQP	EXMHPE	ME	FDUNGFQ	FA	EAYQ
20	DPYO	L	SFYOCPO	DWLGOD	LD	ECTMFEP	EZ	DZXP
21	COXN	K	REXNBON	CVKFNC	KC	DBSLEDO	DY	CYWO
22	BNWM	J	QDWMANM	BUJENB	JB	CARKDCN	CX	BXVN
23	AMVL	I	PCVLZML	ATIDMA	IA	BZQJCBM	BW	AWUM
24	ZLUK	H	OBUKYLK	ZSHCLZ	HZ	AYPIBAL	AV	YVTL
25	YKTJ	G	NATJXKJ	YRGBKY	GY	ZXOHAZK	ZU	XUSK

In this case, the plaintext bounds out as occupying the fifth line. Encryption of a letter x by a shift n can be described mathematically

$$En(x) = (x + n) \bmod 26$$

Decryption is performed similarly

$$Dn(x) = (x - n) \bmod 26$$

In the above formula, the result is in the range 0…….25. If x+n (or) x-n are not in the range 0……25, we have to subtract or add 26.

A. *Limitations*

- It cannot use special character and numbers.
- Space between two words in the plaintext is not considered as one character.
- It is not case sensitive.
- All the 25 possible keys can be tried for the easy identification of the plaintext.

III. RELATED WORKS

Sourabh Chandra et al., proposed a content-based symmetric key method. To encrypt the plaintext, it uses various techniques like binary addition operation, folding method and a circular bit shifting operation [6].

Benni Purnama et al., modified the Caesar cipher method that produces ciphertext that can be read. Replacing the alphabet into two different parts, vocals were replaced by alphabet vocal too and consonant alphabet was replaced by consonantal alphabet. From the test results obtained ciphertext that can be read, then the cryptanalyst not mistrustful of the message [7].

Priyadarshini Patil et al., implemented and analyzed to show an overall performance among popularly used cryptographic algorithms AES, DES, RSA, blowfish and 3DES [8]

Kashish Goyal et al., modified the traditional Caesar cipher. In this method fixed the key size as one and alphabet index is checked. If the alphabet index is odd, decrease the key value by one else increase the value by one [9]

Enas Ismael Imran et al., developed an encryption technique which uses three various methods. Each letter in the plaintext is replaced by some fixed number of position down the alphabet. From the result, data which is encrypted and be decrypted to its readable form [10].

Somdip Dey et al., presented a new combined symmetric-key cryptographic method STJA which is basically based on generalized modified Vernam Cipher, modified Caesar Cipher, NJJA and MSA. To make the crypto system very hard to break, it also used generalized modified Caesar Cipher method, and then they applied TTJSA method [11].

From the above survey, various symmetric key methods are developed to provide the security to the data over network. In this paper, proposed a modified Caesar cipher symmetric method to simply encode the message for preserving privacy. It is very difficult to understand the ciphertext and find out the original message.

IV. PROPOSED SYMMETRIC KEY CRYPTOGRAPHY METHOD

The proposed method is an improvement over the age old existing Caesar cipher. It can accept Alphabets (capital letters and small letters), Numbers and Special characters in the plaintext. It introduces key value in encryption of the Caesar Cipher. The newer formula used in encryption brings new symbols in the output stream of ciphers. The proposed method accepts ASCII character from 0 to 255. So that the number 256 used in the proposed formula both encryption and decryption. It looks complicated than the output generated by the available Caesar Cipher.

A. Encryption Algorithm

Step 1: Generate the ASCII value (p) of the plaintext letter.
Step 2: Generate the octal value corresponding ASCII value. It is considered as a key (k).
Step 3: To apply the formula:
E = (p + k) mod 256
p – Plaintext, k – Key.
Step 4: Generate the ASCII character of the corresponding decimal value resulted from the formula which would be the ciphertext.

B. Decryption Algorithm

Step 1: Generate the ASCII value (c) of the ciphertext character.
Step 2: Here the same encryption key (k) used.
Step 3: To apply the below given formula:
D = (c – k) mod 256
c – Ciphertext, k – Key
Step 4: Generate the ASCII character of the corresponding decimal value generated by the decryption formula. This would be the original plaintext.

C. Advantages of Proposed Method

- The Algorithm is very simple in nature.
- The user can easily encrypt and decrypt the combination of alphabets, numbers and special characters efficiently.
- It considers the space between two words in plaintext as one character.
- It is case sensitive.
- To compare with the existing algorithms, it is very difficult to find the Plaintext from Ciphertext.

D. Illustration

Encryption Process

Let, the character is "X". Now according to the steps we will get the following:

Step 1: ASCII of "X" is 88 in decimal.
Step 2: The octal value of 88 is 130. The value 130 is considered as a key.
Step 3: Apply the following formula
E = (p + k) mod 255
= (88+130) mod 256
= 218
Step 6: As per the algorithm the ciphertext would be " ┌ ".

Decryption Process

After encrypting "X" we have got " ┌" as the ciphertext. Now according to decryption algorithm let's try to get back the original text i.e. "X".

Step 1: 218 is the ASCII value of the ciphertext character " ┌ ".
Step 2: Here, Same key "130" is used.
Step 3: The formula is applied to the ASCII value 218 of the ciphertext character and key 130.
D = (c - k) mod 255
= (218 – 130) mod 256
= 88
Step 4: "X" is the ASCII character of the decimal 88. Character "X" would be the original plaintext.

E. Example Results of the Proposed Method

Plaintext as Single word - Scientist
Ciphertext - ╬≥ö◙↑▬↑

Plaintext as Phrase - Former President of India
Ciphertext - ♀¶◘÷¶H╚¶÷▬ô÷◙↑H♀°H╕◙⌠î

Plaintext as Sentence
A.P.J Abdul Kalam is one of the most distinguished scientists of India.
Ciphertext -
ªf╚f╠Hª≡⌠→♠H╝ε♠ε◘H▬H♀◙÷H♀°H↑■÷H◘♀▬↑H⌠▬↑◙·
→▬■÷⌠H▬≥ö◙↑▬↑▬H♀°H╕◙⌠îf

Plaintext with special characters
A. P. J. Abdul Kalam (15 October 1931 – 27 July 2015), was the “11th President of India” from 2002 to 2007.

Ciphertext
ªfH▄fH╢fHª≡⌠♠H╝ε♠ε◘HZnvH─≥↑♀≡÷¶HnÇrnHdHpzH╢
→♠$Hplnv\bH$ε━H↑■÷HLnn↑■H▄¶÷━ô÷◙↑H♀°H╕◙⌠îL
H°¶♀◘HpllpH↑♀Hpllzf

V. IMPLEMENTATION

The proposed method implemented with ‘C’ Programming Language. The following screenshots shows the sample input to the proposed method and output produced by the developed method.

A. Screenshots

The author Dr. M. Ilayaraja has completed his doctoral degree in the area of data mining. He has been very much interest in doing research in the area of data mining and network security. He was published various papers related to heart disease prediction and information security. He has been familiar in working with some of the data mining tools. He also developed some methods to predict the risk of heart diseases by analyzing large volume of medical datasets and also developed various methods to secure the information over public transmission medium.

Fig. 2 Input File

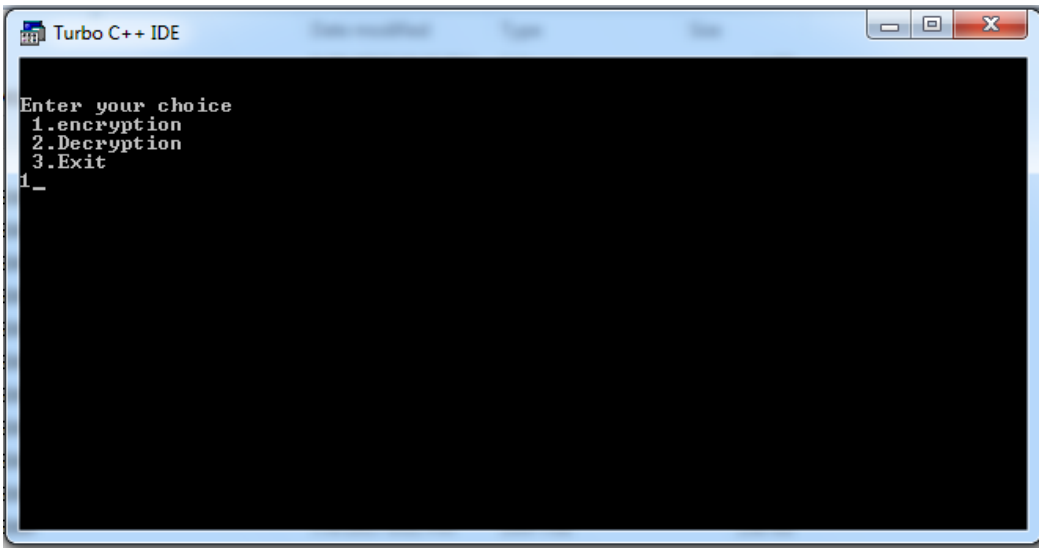

Fig. 3 Encryption Option

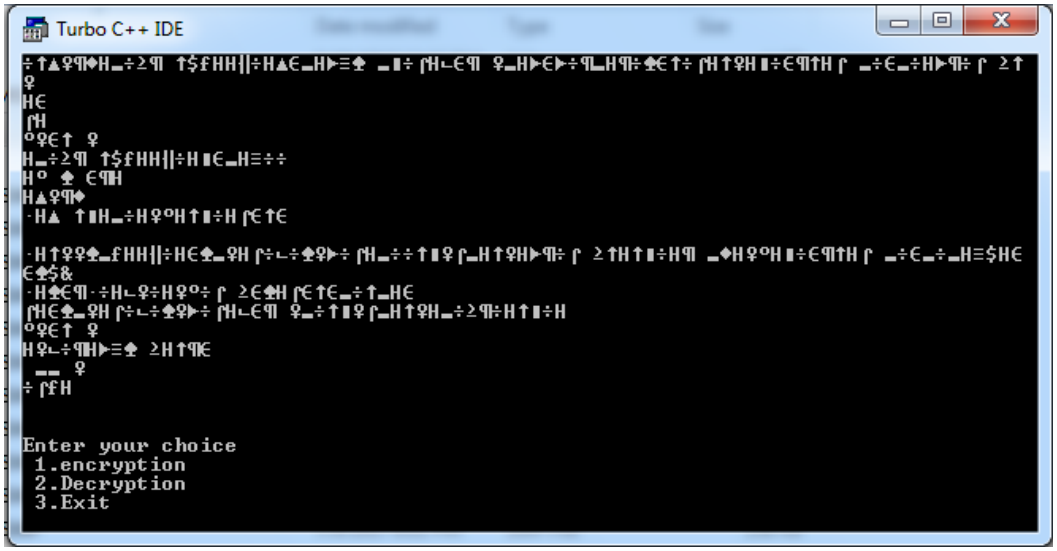

Fig.4 Ciphertext

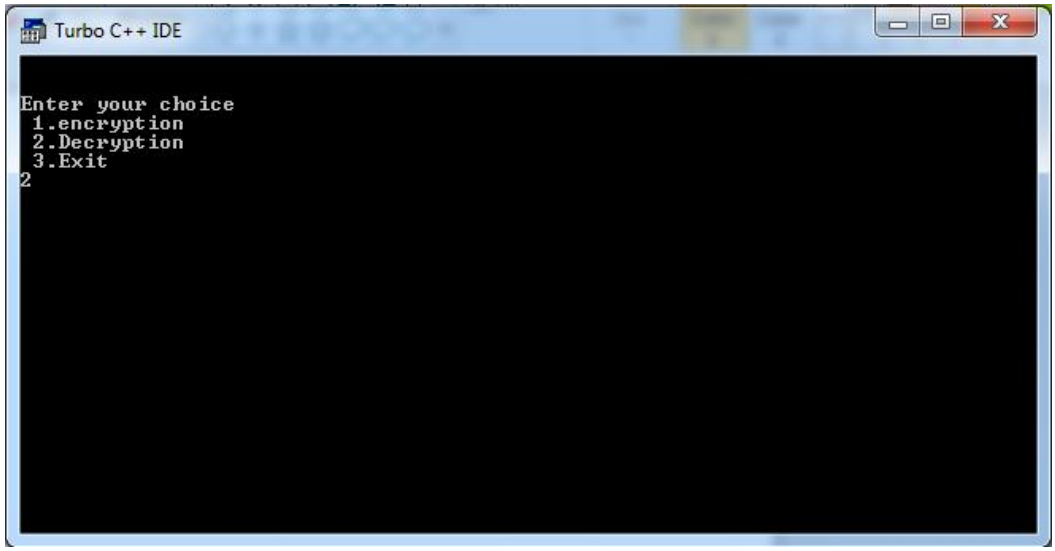

Fig.5 Decryption Option

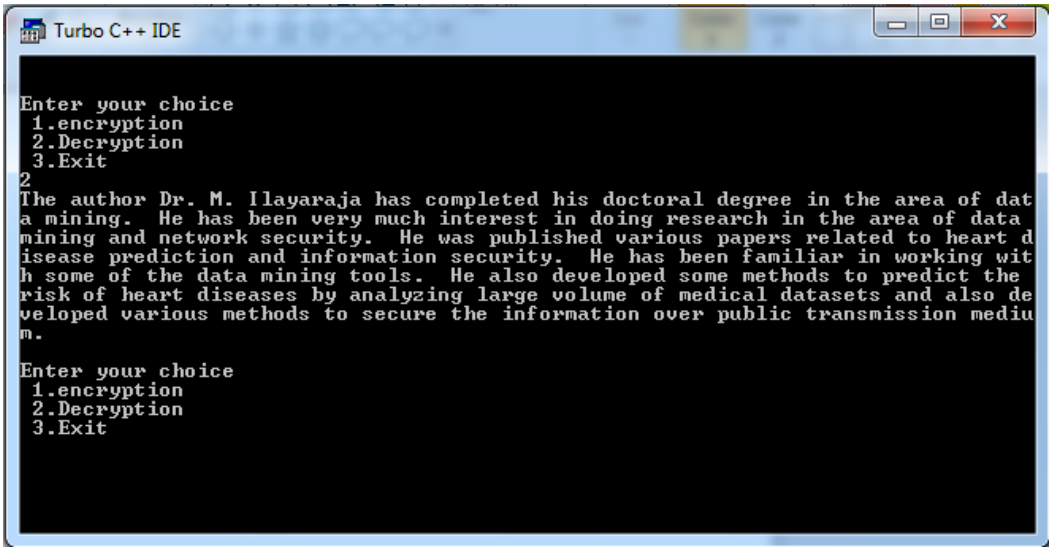

Fig.6 Plaintext

VI. CONCLUSION

Information Security has become a very critical part of modern computing systems. Day by day internet users are growing rapidly. So that, it is necessary to secure the data over public transmission medium. To provide security to data different encryption methods can be used. The proposed method is a refinement of existing Caesar cipher method overcoming the drawbacks of the method. The concept of key is introduced with Caesar cipher to generalize the encryption concept. The ciphertext generated by the proposed method is very hard to understand because of it contains lot of symbols. This is further extended to complicate the age old basic method to a cumbersome method inorder to complicate ciphertext.

REFERENCES

[1] Andrew S. Tanenbaum, Networks Computer, 5th edition, Pearson Education, ISBN-10: 0132553171.
[2] William Stallings, "Cryptography and Network Security: Principles and Practice", 4th Edition, Prentice Hall, 2006.
[3] Hans Delfs and Helmut Knebl, "Introduction to Cryptography: Principles and Applications", Springer International Edition.
[4] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications (0975 – 8887), Volume.1, No.15.
[5] Behrouz A. Forouzan, "Data Communications and Networking", 4th Edition, McGraw-Hills, 2006.
[6] Sourabh Chandra, Bidisha Mandal, Sk. safikul Alam and Siddhartha Bhattacharyya, "Content based double encryption algorithm using symmetric key cryptography", Procedia Computer Science , Vol.57, pp.1228 – 1234, 2015.
[7] Benni Purnama and Hetty Rohayani.AH, "A New Modified Caesar Cipher Cryptography Method with Legible Ciphertext From A Message To Be Encrypted", Procedia Computer Science, Vol.59, pp.195 – 204, 2015.
[8] Priyadarshini Patila, Prashant Narayankar, Narayan D G and Meena S M, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", Procedia Computer Science, Vol.78, pp.617 – 624, 2016.
[9] Kashish Goyal and Supriya Kinger, "Modified Caesar Cipher for Better Security Enhancement", International Journal of Computer Applications, Vol.73, No.3, 2013.
[10] Enas Ismael Imran and Farah abdulameerabdulkareem, "Enhancement Caesar Cipher for Better Security", IOSR Journal of Computer Engineering, Vol.16, Issue.3, pp.01-05, 2014.
[11] A. Somdip Dey1, B. Joyshree Nath2 and C. Asoke Nath, "Modified Caesar Cipher method applied on Generalized Modified Vernam Cipher method with feedback, MSA method and NJJSA method: STJA Algorithm", 2012.
[12] M. Ilayaraja and T.Meyyappan, "Mining Medical Data to Identify Frequent Diseases using Apriori Algorithm", IEEE, 2013.

K.Shankar is an assistant professor in the Department of Computer Science and Information Technology at the Kalasalingam University, Krishnankoil, Tamilnadu, India. He received his master degrees of Master of Computer Applications, Master of Philosophy in Computer Science and Ph.D. degree in computer science from Alagappa University, Karaikudi, India. He has several years of experience working in the research, academia and teaching. His current research interests include Cryptography and Network Security, Cloud security, Image Processing and Soft Computing Techniques.

The author Dr. M. Ilayaraja, Assistant Professor, Department of Computer Science & Information Technology, Kalasalingam University, Krishnankoil. He has completed his doctoral degree in the area of data mining. He has been very much interest in doing research in the area of data mining and network security. He was published various papers related to heart disease prediction and information security. He has been familiar in working with some of the data mining tools. He also developed some methods to predict the risk of heart diseases by analyzing large volume of medical datasets and also developed various methods to secure the information over public transmission medium.

G. Devika is an assistant professor in the Department of Computer Science and Information Technology at the Kalasalingam University, Krishnankoil, Tamilnadu, India. She received her Ph.D. degree in computer science from Anna University, India. She has several years of experience working in the research, academia and teaching. Her current research interests include Cryptography and Network Security, Cloud computing, and Image Processing.