CLCT: Cross Language Cipher Technique

Laukendra Singh(✉) and Rahul Johari

University School of Information and Communication Technology,
Guru Gobind Singh Indraprastha University, New Delhi, India
laukendrasingh.ipu@gmail.com, rahul@ipu.ac.in

Abstract. Information Security has become an important issue in data communication. In modern world, internet and network applications are growing fast. So the importance and the value of the exchanged data over the internet or other media types are increasing. Any loss or threat to information can prove to be huge loss to the organization. Encryption technique is the best solution against the intruder. In this paper we formalize a new symmetric cryptographic cipher technique which is easy to understand and implement. This introduced cipher technique's name is Cross Language Cipher technique (CLCT). In this technique we use the concept of cross language which plays an important role in data security. Today most of the cipher techniques work with English language but we use two languages English and Hindi in our cipher technique. Basically, here are two functions in CLCT; first replaces/converts the English text data to Hindi text data and second function encrypt the Hindi text data. The encryption function is similar to Caesar cipher's function. To find the actual plaintext by intruder is not an easy task because CLCT uses diffusion property. So, CLCT is more reliable and powerful cipher technique. Most of cipher techniques have issue of higher performance and good security feature. Advantages of CLCT are that its performance is high and is less vulnerable to network attack.

Keywords: Cryptography · Encryption · Decryption · Security · Cipher · CLCT · Diffusion

1 Introduction

1.1 Cryptography

Security is the most challenging aspects in the internet and network applications. We need to secure the data in data communication whether the mode of communication is wired or wireless. Basically data security means protecting its confidentiality, integrity, and availability [1]. The consequences of a failure to protect any of the three aspects will incur loss in business, loss of company's goodwill. Organizations are spread across states and countries. Organizations use internet as a backbone to carry out their day to day operations including sensitive data transfer. There is a need to protect customer data as mandated by security controls. So organizations have to pay a huge price in case of compromise of data, especially customer's confidential data. With the rapid growth of information technology and science of encryption, an innovative area for cryptographic products has evolved. The better solution to offer the necessary

J.H. Abawajy et al. (Eds): SSCC 2015, CCIS 536, pp. 217–227, 2015.
DOI: 10.1007/978-3-319-22915-7_21

protection regarding data is cryptography. Many definitions of cryptography are given by authors in their research papers and text books. For the sake of completeness and clarity some of them are listed as follows: "Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attack" [2]. "Cryptography is the subdivision of cryptology in which encryption/decryption algorithms are designed to guarantee the security and authentication of data" [3]. Figure 1 provides a better understanding regarding cryptography. Cryptography is further classified into private key cryptography and public key cryptography.

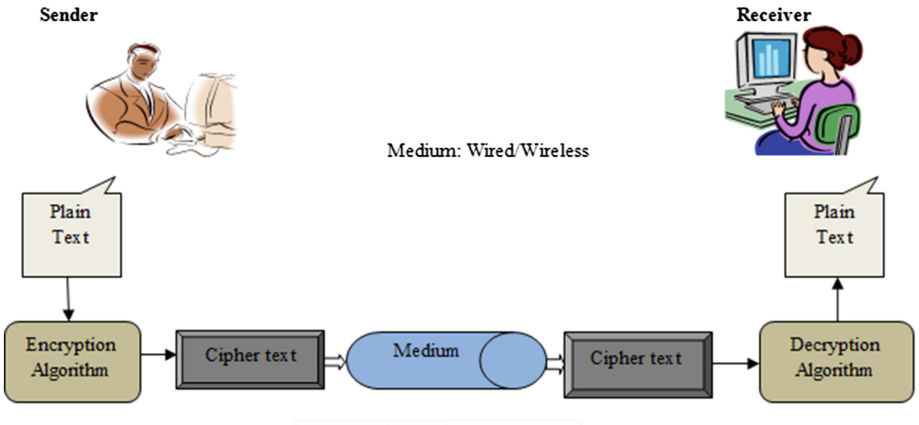

Fig. 1. Concept of cryptography

Private Key Cryptography. In private key cryptography system sender and receiver share a single private key which is used to encrypt and decrypt messages. The algorithm used for private key cryptography is called symmetric key algorithm. Symmetric key algorithm is also divided in two types; stream cipher and block cipher. Stream ciphers encrypt the information bit by bit and Block ciphers encrypt the bits of information block by block.

Public Key Cryptography. Public key cryptography uses the pair of keys one is secret key and other is public key in which one is used for encrypting the message and other is used for decrypting the message.

1.2 What is Cipher?

In cryptography, a cipher is an algorithm for performing encryption or decryption – a series of well-defined steps that can be followed as a procedure [4]. Most of modern ciphers can be categorized in several ways:

- By whether they work on blocks of symbols usually of a fixed size called Block Cipher, or on a continuous stream of symbols called Stream Cipher.
- By whether same key is used for both encryption and decryption called symmetric algorithm, or if a different key is used for each called asymmetric key algorithm. Key must be known to sender and recipient and no one else. Asymmetric key algorithm has public-private key property and one of the key may be made public without loss of confidentiality.
- Ciphers are also categorized as follows [Fig. 2]:

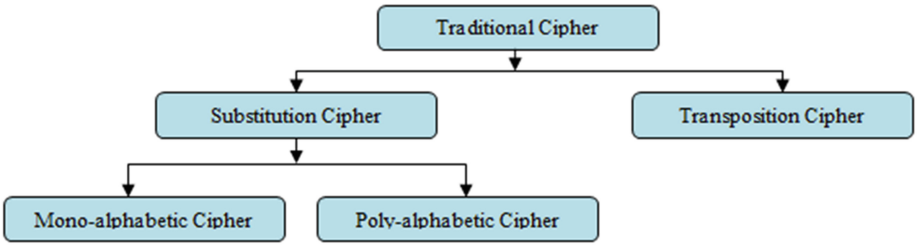

Fig. 2. Categories of ciphers

1.2.1 Substitution Cipher

In Substitution Cipher, one symbol is substituted by other symbol.

Mono-alphabetic Cipher: In mono-alphabetic, a symbol or character in the plaintext is always changed to the same symbol or character in the cipher text regardless of its position in the text. The relationship between symbols in plaintext and cipher text is one-to-one.

Poly-alphabetic Cipher: Whereas in the Poly-alphabetic Cipher, each occurrence of symbol in plaintext can have a different substitute in cipher text. The relationship between the symbols in plaintext and symbols in cipher text is one-to-many.

1.2.2 Transposition Cipher

There is no substitution of characters in transposition cipher; instead their location change. In other words, a transposition cipher reorders or permutes the symbols in a block of symbols.

1.3 Architecture of Cipher

An encryption scheme has five ingredients:

Plaintext: This is the actual readable text or message that is fed into the algorithm as input.

Encryption Algorithm: The algorithm performs various transformation and substitution on the plain text.

Secret/Public Key: Secret key is also an input to the symmetric encryption/decryption algorithm and private-public key combination is used in a asymmetric encryption/decryption algorithm. The key value is independent of the plaintext and cipher text. The algorithm produces the result as output depending on that particular key being used at that time.

Cipher Text: This is an unreadable text or message produced from Encryption algorithm as output. It depends on plaintext and secret/public keys. For a given message, two different keys will generate two different cipher text.

Decryption Algorithm: This algorithm is reverse of encryption algorithm. It takes the cipher text and secret/public keys as inputs and produces the original plaintext.

1.4 Basic Requirement for Secure Encryption

There are two basic requirements for secure use of encryption:

- Sender and receiver must have exchanged copies of the secret/private key in a secure fashion and must keep the key secure.
- We need a strong encryption algorithm. We would like an algorithm to be such that an opponent should be unable to decrypt the cipher text or discover the key.

2 Related Work

In [3] author(s) demonstrate the comparative performance analysis of MD5, DES and AES encryption algorithms on the basis of execution time, LOC (Lines of Code) over a web application. In [5] author(s) discusses and analyses the current developments in online authentication procedures including one-time-password systems, biometrics and Public Switched Telephone Network for cardholder authentication. The author(s) proposes a complete new framework for both onsite and online (Internet shopping) credit card transactions. In [6, 9] author(s) presents a detailed review on various types of vulnerabilities, Structured Query Language Injection attacks, Cross Site Scripting Attack, and prevention techniques. The Author(s), also proposes future expectations and possible developments of countermeasures against Structured Query Language Injection attacks. In [7] author(s) presents an integrated model to prevent reflected cross site scripting attack and SQL Injection attacks in applications which are made in PHP. These models work in two modes which are production and safe mode environment. They create sanitizer model for reflected cross site scripting attack and security query model for SQL Injection attack in safe mode. They validate user input text against sanitizer model and input entries which create SQL queries are validated against security query model in production mode. In [8] author(s) demonstrates the vulnerabilities and network attacks pertaining to cryptographic algorithms such as AES, DES

and MD 5 et al. In [10] author(s) also proposes a similar technique to handle the security of the alphabets and numbers but without any detailed comparison. In [11] author(s) proposes a technique to encrypt and decrypt the Alphabets, Numbers and Alphanumeric data in minimum span of time with minimum lines of code, designed logic of which has been coded in JAVA In [12] author(s) have designed a Java based tool to show the exploitation of Injection using SQL Injection attack and Broken Authentication using Brute Force Attack and Dictionary Attack and the prevention of all these attacks by storing the data in our database in encrypted form using AES algorithm. In [13] author(s) have explored prevalent system vulnerabilities such as Password Ageing, Empty String Password, Empty Catch Block Problem etc. and network attacks such as Brute force attack, Denial of service Attack and Dictionary Attack etc.

3 Proposed Work

In modern World, web and network applications are growing fast. So security is the most challenging aspects in the web and network applications. By keeping it in mind, we introduce a new cipher technique. This new introduced cipher technique is known as Cross Language Cipher Technique (CLCT). CLCT is easy to understand and implement. Mostly cipher techniques work with English language. So, in this cipher technique we use the concept of cross language which provides an important role in data security. We use two languages like English and Hindi in our cipher technique. CLCT uses multiple functions at both the side sender and receiver. The actual input text is written in English language. First function of CLCT encodes the characters of English language into their corresponding ASCII value. Second function represents the corresponding ASCII value of English language characters to ASCII value of Hindi language characters. The representation of characters is manually defined. Third function is the actual encryption function which encrypts the particular data or information with the help of key. Fourth function starts to work when it gets output from the encryption function. It decodes the received data or information into Hindi language text. The output from the decode function is the actual cipher text which is sent to the receiver. The reverse steps are applied at receiver side to get the actual plain text.

3.1 Description of Algorithm

Working steps of the algorithm at both side sender and receiver are defined in following.

3.1.1 Sender Side

Steps that are performed at sender side are defined as follows:

1. Take the input text from a text file (MY.txt) in English language.
2. Encode the text into ASCII value.
3. Represent/convert the encoded text into ASCII value text of Hindi language.
4. Store the converted text into MY1.txt file.

5. Split the string (text) into characters.
6. Applying encryption algorithm.
7. Merge the characters into string after encryption.
8. Decode the string (text) into Hindi language text.
9. Store the actual cipher text (decoded text) into MY2.txt file.
10. Send the cipher text to the receiver.

Flow diagram of desired CLCT technique at sender side is shown in Fig. 3.

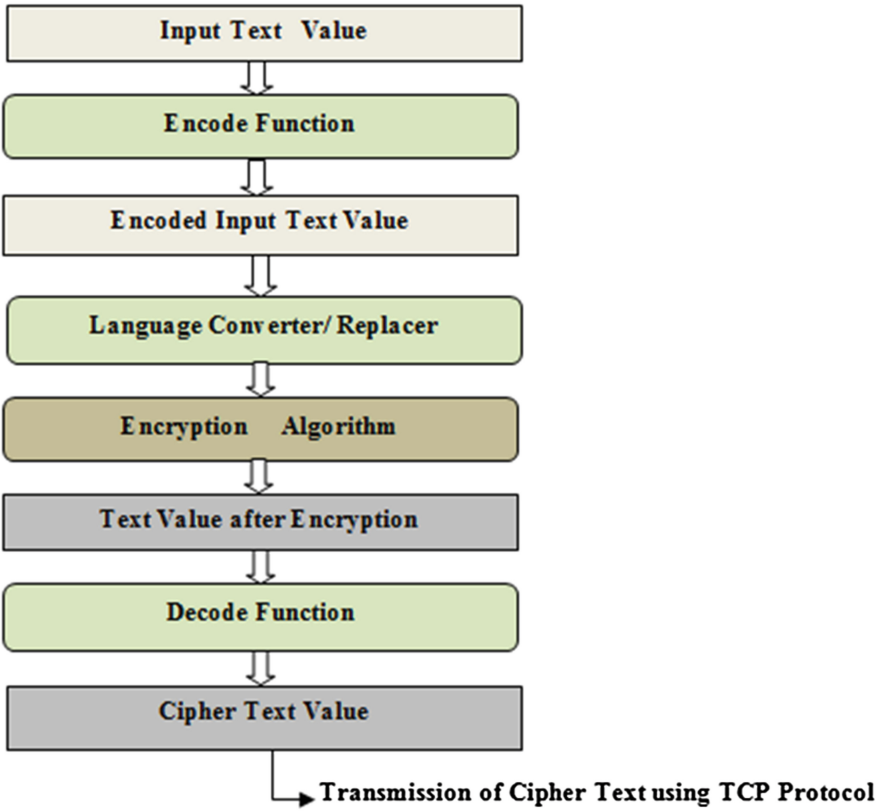

Fig. 3. CLCT cipher encryption at sender side.

Input Text Value: The value of this field is simply a text which is written in English language format. This is the actual input text.

Encode Function: Encode function encodes the input text data into their corresponding ASCII value.

Encode Input Text Value: This is a ASCII value received from the output of Encode Function and saved in a file.

Language Replacer/Converter: This body of the CLCT algorithm plays an important role. Function of this body represents the ASCII value of English language text data to the ASCII value of Hindi language text data. This is a manual representation.

Encryption Algorithm: This is the actual encryption function which is similar to Caesar cipher. Input text data to this function is encrypted to another text data which is known as cipher text. But this is not the actual cipher text of CLCT cipher technique.

Text Value After Encryption: This field defines the cipher text value which is obtained after performing encryption algorithm.

Decode Function: This function decodes the received text data into Hindi text data.

Cipher Text Value: This is the actual cipher text data/value is stored in a file.

Now Sender sends the cipher text data to the Receiver.

3.1.2 Receiver Side

Steps that are performed at receiver side are defined as follows:

1. Take the cipher text as input.
2. Encode the received text data into their corresponding ASCII value.
3. Store the encoded text data.
4. Split data text into characters.
5. Apply the decryption algorithm.
6. Merge the characters into string after decryption.
7. Decode the string into Hindi language text.
8. Replace/Convert the Hindi text data to the required English text.

Flow diagram of desired CLCT cipher technique at receiver side is defined in Fig. 4.

Example: Encrypt the message “CRYPTOGRAPHY” using CLCT.

Solution: Table 1 illustrates the concept of CLCT technique for the given input text.

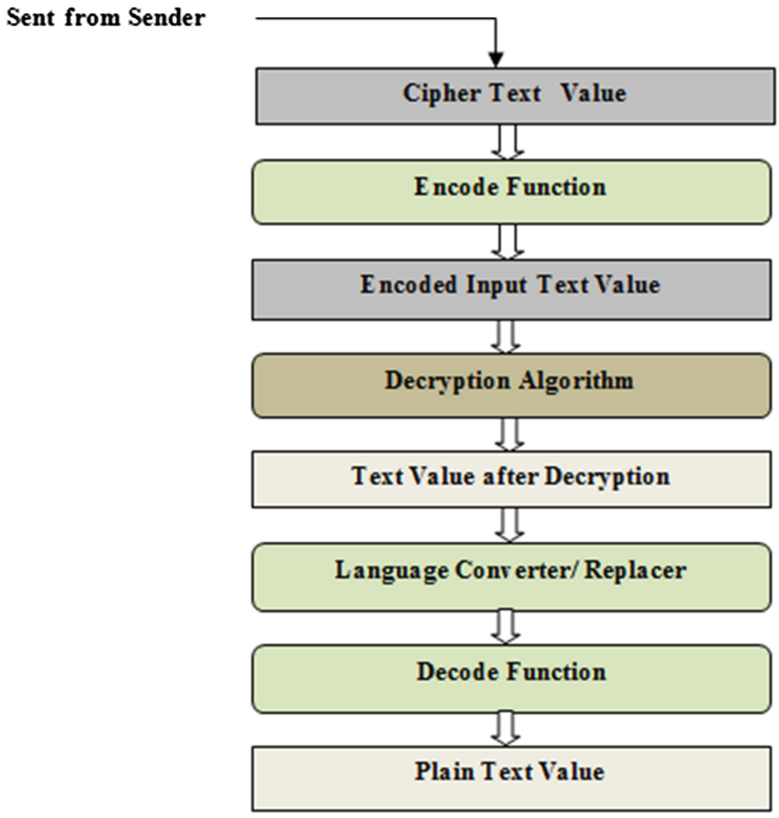

Fig. 4. CLCT cipher decryption at receiver side.

Table 1. CLCT algorithm with Encryption and Decryption at Sender side and Receiver side respectively

Sender Side	Receiver Side
1. Plain Text: CRYPTOGRAPHY	**6.** Plain Text: CRYPTOGRAPHY
2. Input text to Encode Function: CRYPTOGRAPHY	**5.** Decode Function decodes the received text from Language Replacer/Converter into English language text format. This is the actual plain text of CLCT technique.
3. Output text from Encode Function and input to Language Replacer/Converter: CRYPTOG RAPHY	**4.** Output text from Decryption Function and input to Language Replacer/Converter: चरयपतो गरअपहय
4. Output text from Language Replacer/Converter and input to Encryption Function: चरयपतो गरअपहय	**3.** Output text from Encode Function and input to Decryption Function: तऺहऴमॕ डऺएऴृह
5. Decode Function decodes the received text from Encryption Function into Hindi language text format. This is the actual cipher text of CLCT technique.	**2.** Input text to Encode Function: त□ह□म□ड□एक्ह
6. Cipher Text: त□ह□म□ड□एक्ह	**1.** Cipher Text: त□ह□म□ड□एक्ह

4 Simulation

We have used NetBeans IDE 7.1 as simulator for implementation of CLCT technique. The reason for using the NetBeans IDE is that, it is open source. The code has been written entirely in java programming language because besides being open source it offers the flexibility of easy to code cryptographic functions. The snapshots are illustrated in Figs. 5 and 6.

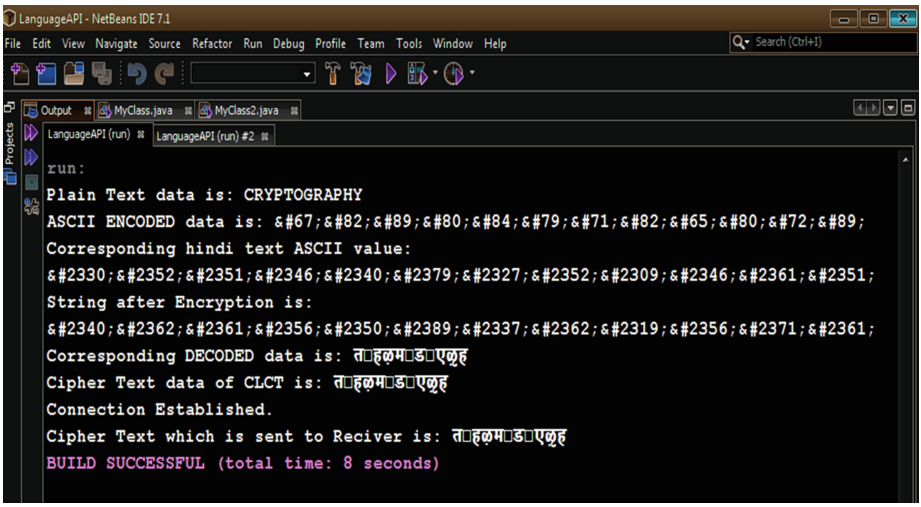

Fig. 5. CLCT at sender side

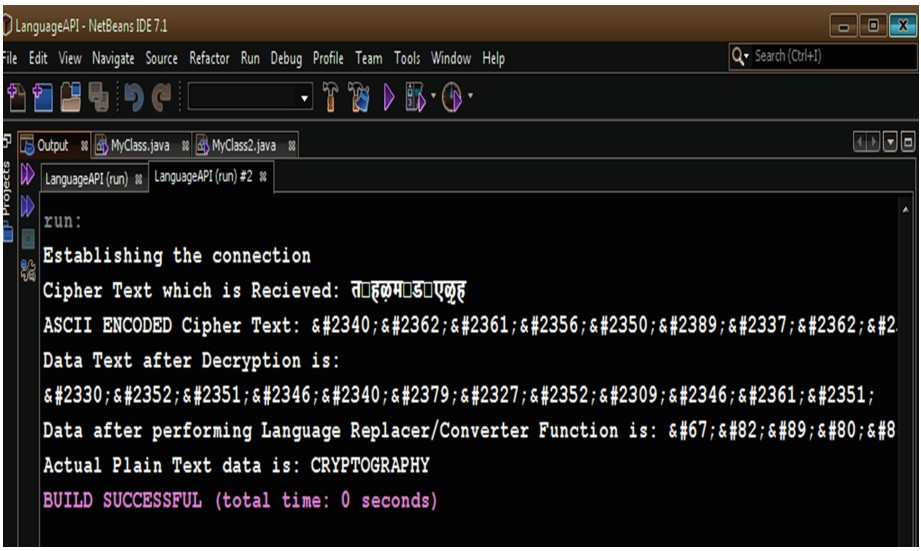

Fig. 6. CLCT at receiver side

5 Analysis

Today most of the cipher techniques in the literature are designed and developed in the English Language, but the introduction of this new cross language cipher technique of converting plaintext from the English to Hindi language would make the resultant cipher text robust, computationally strong and more secure to various attacks such as BruteForce Attack, Man in the Middle Attack, Birthday Attack, Replay attack et al. making it difficult for the hackers and crackers to decode it.

6 Conclusion and Future Work

We have successfully implemented our proposed CLCT technique. The cipher Text obtained is safe, reliable and secure. In future work, instead of converting Plain Text (in English language) to Cipher Text (in Hindi language) it can be mapped/converted to other regional languages like Assamese, Bengali, Oriya, Tamil and Telugu. Also we propose to compare other results of CLCT technique with other cryptographic techniques such as Additive cipher, Affine cipher, Vigenere cipher, Rail Fence cipher, Hill cipher et al. on the parameters such as LOC (Line of Code), space and time complexity etc.

References

1. Forouzan, B.A.: Cryptography and Network Security. Mc. Graw-Hill, Special Indian Edition, New Delhi (2007)
2. Chaudhari, M.P., Patel, S.R.: A survey on cryptography algorithms. Int. J. Adv. Res. Comput. Sci. Manage. Stud. **2**(3), 100–104 (2014)
3. Ebrahim, M., Khan, S., Bin Khalid, U.: Symmetric algorithm survey: a comparative analysis. Int. J. Comput. Appl. **61**(20), 12–19 (2013)
4. Johari, R., Jain, I., Ujjwal, R.L.: Performance analysis of MD5, DES and AES encryption algorithms for credit card application. In: International Conference on Modeling and computing (ICMC – 2014) (2014)
5. Gupta, S., Johari, R.: A new framework for credit card transactions involving mutual authentication between cardholder and merchant. In: 2011 International Conference on Communication Systems and Network Technologies (CSNT), pp. 22–26. IEEE (2011)
6. Johari, R., Sharma,P.: A survey on web application vulnerabilities (SQLIA, XSS) exploitation and security engine for SQL injection. In: 2012 International Conference on Communication Systems and Network Technologies (CSNT), pp. 453–458. IEEE (2012)
7. Sharma, P., Johari, R., Sarma, S.S.: Integrated approach to prevent SQL injection attack and reflected cross site scripting attack. Int. J. Syst. Assur. Eng. Manage. **3**(4), 343–351 (2012). Springer
8. Ahuja, S., Johari, R., Khokhar, C.: CRiPT : cryptography in penetration testing. In: Springer's AISC Series for International Conference on Computer and Communication Technologies - IC3T (to appear 2015)
9. Johari, R., Gupta, N.: Secure query processing in delay tolerant network using java cryptography architecture. In: 2011 International Conference on Computational Intelligence and Communication Networks (CICN), pp. 653–657. IEEE (2011)

10. Ruby, L., Johari, R.: Designing a secure encryption technique for web based application. Int. J. Adv. Res. Sci. Eng. (IJARSE) **3**(7), 159–163 (2014)
11. Ruby, L., Johari,R.: SANE :Secure encryption technique for alpahamuneric data over web based applications. Int. J. Eng. Res. Technol. (IJERT) 3(8) (2014)
12. Jain, I., Johari, R., Ujjwal, R.L.: CAVEAT: credit card vulnerability exhibition and authentication tool. In: Second International Symposium on Security in Computing and Communications (SSCC 2014), pp 391–399 Springer (2014)
13. Ahuja, S., Johari, R., Khokhar, C.: EAST: Exploitation of Attacks and System Threats in Network. In: Mandal, J.K., Satapathy, S.C., Sanyal, M.K., Sarkar, P.P., Mukhopadhyay, A. (eds.) Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing (AISC Series), vol. 339, pp. 601–611. (2015)