Implementation of Tangent and Cotangent rules to Provide Security in E-communication

[1]Narander Kumar
Department of Computer Science
B. B. Ambedkar University
Lucknow (U.P.), 226025,INDIA

[2]Vishal Verma
Department of Computer Science,
B. B. Ambedkar University
Lucknow (U.P.), 226025,INDIA

[3]Vipin Saxena
Department of Computer Science,
B. B. Ambedkar University
Lucknow (U.P.), 226025, INDIA

ABSTRACT

In the data communication, the intriguing issue to provide data security and these led to comprise the many areas including the impregnable medium and trusted third party to maintain a database and various types of encryption techniques. These are main inducement of researchers in this area to protect the data from unauthorized users for malicious purpose. Therefore there are requires the different types of encryption and decryption techniques to secure the data. In the proposed paper, there are used the Tangent and Cotangent rules to generate the cipher and decipher at sending and receiving ends respectively. At the sending side, take the message alphabets which message want to communicate through electronic communication and find the corresponding values of alphabets from standard alphabetical table and apply the rules of Tangent. Find the corresponding values of Tangent of a particular alphabet and use this value as cipher at sending end. At the receiving end, there are taking the value of Cotangent of those particular receiving alphabets. Finally, get the value of same alphabets. This paper provides an algorithm as well as validates the proposed mechanism through UML Diagram.

Keywords: Tan x, Cot x, cipher/decipher, e-communication, UML.

1. INTRODUCTION

The rapid devolvement of internet and secure transmission of personalized and secure transmission of data may lead the attention in this area. Data security issue of electronic data communication incorporates the different area including secure medium for communication, effective encryption techniques and trust based third party for maintaining the database [1] rapid use of hand-handled device like smart mobile phones, (PDA) personal digital assistance as well as application such as a e-payment, secure messaging etc need more security than conventional security [2]. Since there are various use of digital devices and advance applications which involve in financial transaction and transfer the secure data through electronic communication. Electronic communications means when data is in the route, in order to protect the data from going into the hands of an unauthorized person who may have alter the data for malicious person[3] now a day's sharing the secure data or importance over internet is growing a critical issue due to security problems[4].Therefore there is a need of different types of techniques which provide the security in different manner in different area of data and information .In present paper, proposed an techniques with use of tangent and cotangent rules to provide the security in e-communication. Through tangent and cotangent rules, there is generating an encryption key and make cipher for transmitting the data at sender side. On the receiver used these rules apply into get back the data in original form, or this can say that with the help of these rules of tangent and cotangent rule we opened the decryption key to decode the cipher data and get the data in original form. Since use of these techniques we take the position value of alphabets for standard alphabet and apply tangent and cotangent rules than we get ciphers and reverse data in the original form. Due to mathematical bits of stream move during the transmission it is comparatively hard to decode the data by unauthorized access or unauthorized uses. In this paper, there are giving an implementation Table as an example as well as UML diagram for validation proposed technique. The organization of paper is as fallows. Section 2 provides the review of work in this line. Section 3 describe the whole methodology or implementation with algorithm as well as implementation Table as an example Section 4 gives the conclusion and future direction also.

2. RELATED WORK

Standard instruction for protecting message, text, audio, video, has been given in [5] and they said that he encryption is nothing it is just like a pencil and paper but it provide message security. Implementation of AES encryption and decryption AES-128has been given in [6]. Used of blowfish and modified version of RSA an encryption and decryption of file at cloud server in given in [7]. Encryption and decryption algorithm with the help of inserting dummy symbol, rotating, transposition complement and inserting dummy special symbol, control byte to build the data and table has been given in [8]. A study of understanding and evolution of different existing data hiding algorithm for encryption is given in [4]. An architecture which helps to encrypt and decrypt the file at user side that provides the security which data is moved is proposed in [9]. A block based transformation algorithm which is based on the combination of image transformation is described in [10]. Two algorithms named 128-bit AES and RSA is implemented in single chip which provide the difficulties to hacker and tracker is describe in [11]. A combination of cryptography and stenography is given in [12]. A method for nested digital watermark embedding and extraction with nested watermark embedded in to the main image to increase the embedded capacity and improve the security level of watermark has been given [13].

Mixed technique is discussed in [14] to secure the database. Since encryption as well as partial image encryption using phase manipulation is given in [15]. Three different image encryption techniques for color image has discussed in [16]. Performance evolution has been given in [17] of encryption

algorithm. Performance comparison of DES, 3DES, Blowfish AES and NTRU is given in [18]. Parametric comparison the various algorithms with TACIT encrypted algorithm is discussed in [19]. An encrypted algorithm which insure the lossless of transmission of image is proposed in [20].Query processing performance over encrypted database with reverse encryption algorithm has been given in [21]. As review of literature, the findings is that there is need of various encryption and decryption techniques for generating the encryption decryption key through apply different mechanism for different type of data to move in the electronic form. The present paper proposed an algorithm use of tangent and cotangent rules, with implementing table as well as UML class diagram for validation the mechanism.

3. ALGORITHM:

The edges of OLAP Data cube which is important data for any business concern and want to communicate using electronic communication. There are need of ciphers which requires for communications. The set of rules of proposed mechanism are as follows:

1. **Initialization**

   Sender finds the alphabets of the message and counts their position in the standard alphabets.

2. **Generation of encryption Key**

   Calculate the value of Tan X, the resultant value send to receiver as a cipher. The encrypted key is the resultant value of Tan X.

3. **Generation of Decryption Key**

   Calculate the value of Cot X, the resultant value is equal to their position in the standard alphabets. This is used as decryption key or decipher at the receiving end.

4. **Decode the original Data**

   Finally, get their original bit pattern which is same as sender end.

Through this algorithm, there are use of the tangent rule as a cipher at the sending side Cotangent rules as decipher at the receiver side, find the totally mathematically cipher which is used in flow of information that are used in communication.

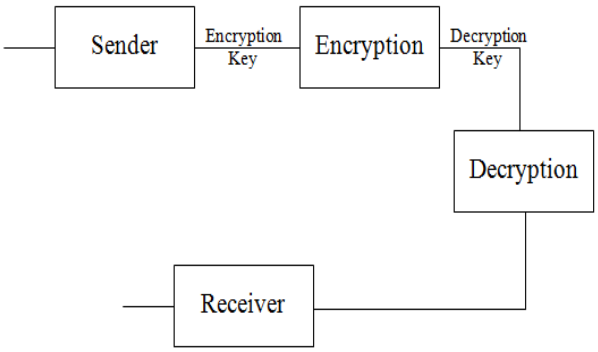

Figure 1: Block Diagram

3.1. Implementation Table 1:

Sender					Receiver
		Ciphers			
Plane text	**X**	**Tan x**	**Cot X**	**X**	**Plane text**
P	16	0.2867	3.487	16	P
O	15	0.2679	3.732	15	O
L	12	0.2125	4.704	12	L
I	9	0.1583	6.313	9	I
C	3	0.0524	19.081	3	C
Y	25	0.4663	2.144	25	Y

Implementation Table 2:

Sender					Receiver
		Ciphers			
Plane text	**X**	**Tan X**	**Cot X**	**X**	**Plane text**
I	9	0.1583	6.313	9	I
N	14	0.2493	4.010	14	N
S	19	0.3443	2.904	19	S
U	21	0.3838	2.605	21	U
R	18	0.3249	3.077	18	R
A	1	0.0174	57.289	1	A
N	14	0.2493	4.010	14	N
C	3	0.0524	19.081	3	C
E	5	0.0874	11.430	5	E

In the above example, we take a simple text and find the alphabetical values in the standard alphabet and find their corresponding values. These corresponding values converted in the ciphers through calculate the value of Tan X, the value of this objective function (Tan X) is send as cipher code of information or in other words as encryption key and at receiving end the encryption key generate by the value of Tan X. At the receiving end calculate the value of Cot X as objective function. The value of this function (Cot X) is equal to the corresponding value of standard alphabets. Finally get the original message.

3.2 UML Class Diagram:

Unified Modeling Languages validate the model. Therefore, to present the validation of proposed model or mechanism is given below.

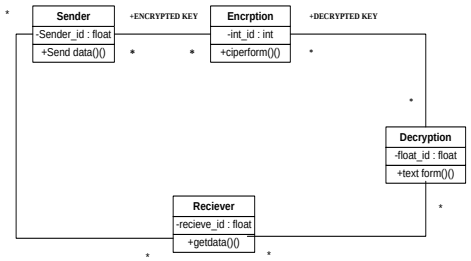

Figure 2: UML Class Diagram

4. CONCLUSIONS AND FUTURE DIRECTIONS:

This paper presents the techniques of use of Tangent and Cotangent rule as cipher and decipher for secure communication. An algorithm presents how does the change a simple message in to cipher code. A unified modeling language class diagram to validate the proposed mechanism or technique. Implementation presents through implements tables which provide the whole procedure of proposed technique for secure e-communication. Since now a day's communications by portable devices like smart phones, PDAs and mobile so this type of mechanism play an important role in communication. For future direction, these proposed rules apply in the different field of areas like generation of different encryption and decryption keys or ciphers.

REFERENCES

[1] Himanshu Gupta and Vinod Kumar Sharma, "Multiphase Encryption: A New Concept in Modern Cryptography" International Journal of Computer Theory and Engineering, Vol. 5, No. 4, pp-238-240, August 2013.

[2] Anjali Patil, Rajeshwari Goudar, "A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices" International Journal of Scientific & Technology Research, Volume 2, Issue 8, pp-61-65, August 2013.

[3] Dr. Mamta Sood, Manohar Wagh, Monika Cheema, " A Review on Various Data Security Techniques in Wireless Communication System" International Journal of Engineering Research and Applications, Vol. 3, Issue 2, pp.883-890, March -April 2013.

[4] Vimal, Mahendra Kumar Patil, "Review of Various Data Hiding Algorithms in Encrypted Images" International Journal of Engineering Research and Development, Volume 7, Issue 6, PP 42-49, June 2013.

[5] ShachiSharma, VintiGupta, "Encryption and Decryption using one PAD time Algorithm in MAC Layer" International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 6, pp-2248-2250, June 2013.

[6] P. Aatheeswaran, Dr.R.Suresh Babu, "FPGA can be implemented by using Advanced Encryption Standard Algorithm" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 1, pp-675-679, jan 2013.

[7] Reema Gupta1, Tanisha, Priyanka, "Enhanced Security for Cloud Storage using Hybrid Encryption" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, pp-2710-2717, July 2013.

[8] TSANG-YEAN LEE, HUEY-MING LEE, HOMER WU, JIN-SHIEH SU, "Data Transmission Encryption and Decryption Algorithm in Network Security" Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, pp-417-422, September 22-24, 2006.

[9] Sanjoli Singla, Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique" International Journal of Advanced Research in Computer Engineering & Technology, Volume 2, Issue 7, pp-2232-2235, July 2013.

[10] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm" International Journal of Computer Science, 35:1, IJCS_35_1_03, IAENG, 19 February 2008.

[11] Suresh M G, Dr. Nataraj K.R, "Advanced Cryptographic System for data Encryption and Decryption" International Journal of Engineering Research & Technology, Vol. 2 Issue 1, pp-1-6, January- 2013.

[12] B. Padmavathi, S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique" International Journal of Science and Research, Volume 2 Issue 4, pp-170-174, April 2013.

[13] Jasdeep Singh Bhalla, Preeti Nagrath, " Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm" International Journal of Scientific and Research Publications, Volume 3, pp-1-6,Issue 4, April 2013.

[14] Sabareesan, Gobinathan, "Network Database Security Issues and Defense" International Journal of Engineering Research and Applications, Vol. 3, Issue 1, pp.1748-1752, January -February 2013.

[15] Parameshachari B D, K M Sunjiv Soyjaudah, Sumitrha Devi K A, " Secure Transmission of an Image using Partial Encryption based Algorithm"International Journal of Computer Applications, Volume 63– No.16, pp-33-36, February 2013.

[16] Rajinder Kaur, Er. Kanwalpreet Singh, "Comparative Analysis and Implementation of Image Encryption Algorithms" International Journal of Computer Science and Mobile Computing,Vol. 2, Issue. 4, pg.170 – 176, April 2013.

[17] Vishwa gupta,. Gajendra Singh ,.Ravindra Gupta, " Advance cryptography algorithm for improving data security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, pp-1-6. January 2012.

[18] Yashpal Mote, Paritosh Nehete, Shekhar Gaikwad, "Superior Security Data Encryption Algorithm (NTRU)" International Journal of Engineering Sciences, Vol. 6, Issue July 2012.

[19] Manmeet Kau1, Manjit Kaur, Gurmohan Singh, "Comparison of TACIT Encryption Algorithm with Various Encryption Algorithms" International Journal of Electronics and Computer Science Engineering, Volume1,Number 2, pp741-750, 2012.

[20] Gamil R.S. Qaid, Sanjay N. Talbar, "Encryption and Decryption of Digital Image Using Color Signal" International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, pp-588-592, March 2012.

[21] Ayman Mousa, Elsayed Nigm, Sayed El-Rabaie, Osama Faragallah, " Query Processing Performance on Encrypted atabases by Using the REA Algorithm" International Journal of Network Security, Vol.14, No.5, PP.280-288, Sept. 2012.

Brief Biography:

Dr. Narander Kumar received his Post Graduate Degree and Ph. D. in CS & IT, from the Department of Computer Science and Information Technology, Faculty of Engineering and Technology, M. J. P. Rohilkhand University, Bareilly, Uttar Pradesh, INDIA in 2002 and 2009, respectively. His current research interest includes Quality of Service (QoS), Software Engineering, Computer Networks, Resource Management Mechanism in the networks for Multimedia Applications, Performance Evaluation and Cloud Computing. Presently he is working as Assistant Professor, in the Department of Computer Science, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, INDIA.

Vishal Verma is a research scholar in Department of Comuter Science, Babashaheb BhimRao Ambedkar University, Lucknow, India. Earlier he got his Master of Computer Application (MCA) from the above University and presently he is working on Data Mining Applications through UML.

Vipin Saxena is a Professor and Head, Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, India. He got his M.Phil. Degree in Computer Application in 1992 & Ph.D. Degree work on Scientific Computing from University of Roorkee (renamed as Indian Institute of Technology, Roorkee, India) in 1997. He has more than 16 years of teaching experience and 19 years of research experience in the field of Scientific Computing & Software Engineering. He has published more than ninety one International and National research papers and authored four books in the Computer Science field. Dr. Saxena is a life time member of Indian Science Congress.