A Security Algorithm for On-Line Analytical Processing Data Cube

[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

The progress of data exchange in the electronic way increases the requirement of data security. Since data security needs more resources to access stored the information this leads to new mechanism and algorithm. Therefore the researcher interest moves to provide different techniques for security concern. There are various mechanisms available in the literature for images and other concern. If there is use of on-line analytical processing (OLAP) data cube then there is lack of techniques or mechanisms in this area. In present work, a Security Encryption Algorithm for On-Line Analytical Processing (SEAOLAP) data cube. Since data cube provided itself is a technique to find the edges for business concern to any system. These edges are the most important data for any business system. The proposed technique is based on the logarithmic properties and power functions. Through these techniques after encryption we send only mathematical data for electronic communication. Only mathematical data is used in E-communication, which provides the strong encryption key to hide the information.

Keywords: OLAP, SEAOLAP, Data Cube, e-communication, UML.

1. INTRODUCTION

Growth of E-communication, security concern is most important for the users. Cryptographic techniques provide the security for the data in communication or air in the signal form, from the hacker or tracker. Increasing the use of E communication data may be financial concern or such typed data which need more securely than (we can say) the man means such type of data which has the edges of business concern needs the security. To provide the security for data, cryptographic techniques play important role to make such techniques. In the continuation for providing the security some new cipher techniques are required. The goal is to make the data secure from unauthorized access [1]. Data cryptography is the scrambling of the content of data like edge of any company, text, audio, video etc to make it unintelligible during transmission. There are database encryption mechanisms [2-5] which provide the verification for the authentic origin of data item. It prevents user from obtaining the unauthorized data and preventing from leaking information database in storage mediums like disc, CD-Rom etc. Since to obtain the security, we store the data in cipher form and for any query solving, decrypt or send the encrypted data and then solve the query which leads to sacrifice the performance usually. The cost of decryption over all the encrypted data is cost effective [6]

In this paper, authors have proposed a new algorithm or technique which provides the security algorithm for (SEAOLAP) on line analytical processing data cube. The technique is based upon the simple concept of the logarithmic function which is used to transfer mathematical data for electronic communication for the edges of data of any company.

2. RELATED WORK

The shared architecture for both encryption and decryption has discussed in [7] through this architecture one can reduce the path delay and path. Shared-secrete-key. Intermediate – key and session-key and matrix operations are used for encoding and decoding the data [8]. The use of RSA algorithm for designing of an encryption mechanism, they use latitude as source and longitude as destination (geographic location) as keys along with the private and public keys [9]. A new Encryption algorithm called REA (reverse encryption algorithm) has proposed in [10] which provide max and control the time cost for encryption and decryption. A parallel encryption model with Byte-Rotation encryption algorithm has discussed in [11] which applied and different blocks of plain text and applies multithreading concept of single processor system to execute in parallel manner. User desired security and processing level based algorithm has proposed in [12] through fuzzy logic used various keys for the encryption/decryption process. A user Interface through Unified Modeling Language has designed in [13] and they have given the strength and weakness of user Interface. To secure routing protocol AODV, a techniques has proposed in [14] which preserved the confidentially and secure data. Increasing security and improve performance, there is use of secret-key block cipher called 64-bit blowfish which has been designed and proposed in [15]. A dual Approach of security and compression, which achieved through Huffman Coding as per their size and type of data has proposed in [16]. A compression between RSA file transfer and secure RSA file transfer are given in [17]. A lager based framework for image encryption has proposed in [18] .Three DNA-based algorithm for parallel subtractor, comparator and modular arithmetic have proposed in [19] to achieve the factor the product of two large prime numbers and breakthrough in basic biological operations using a molecular computer. An array of novel code optimization method has proposed in [20] for increasing the energy consumption efficiency of different security algorithm and proposed some principles for computing with energy constraints.

User performances based adaptive resource management through control algorithm has proposed in [21]. A framework

for OLAP data cube is used to analyze the Vehicle Insurance Policy System (VIPS) and identity the entities for business perspective of vehicle [22]. Utilization DNA sequencing, more secure and reliable transmitting of message is discussed in [23]. An idea of cipher cloud or a framework has proposed in [24] for providing the security in cloud environment. After review has been done in this line, there is a need of an algorithm which provides the security to on line analytical processing data cube. In the present paper, there is a proposed algorithm named security algorithm for an online analytical processing (SEAOLAP) with UML class diagram as well as an implement example through which in the transmission of data is secure.

3. PROPOSED ALGORITHM

The edges of OLAP Data cube which is important data for any company and want to communicate using electronic communication. There are 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 $Y=2^X$ the resultant value send to receiver as a cipher. The encrypted key is the resultant value of $Y=2^X$.

3. Generation of Decryption Key

   Calculate the $Z=\log_2 Y$ the resultant value is equal to their position in the standard alphabets. This is used as decryption key at the receiving end.

4. Decode the original Data

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

Through this algorithm named SEAOLAP data cube, find the totally mathematically cipher which is used in flow of information that are used in communication as shown in figure 1.

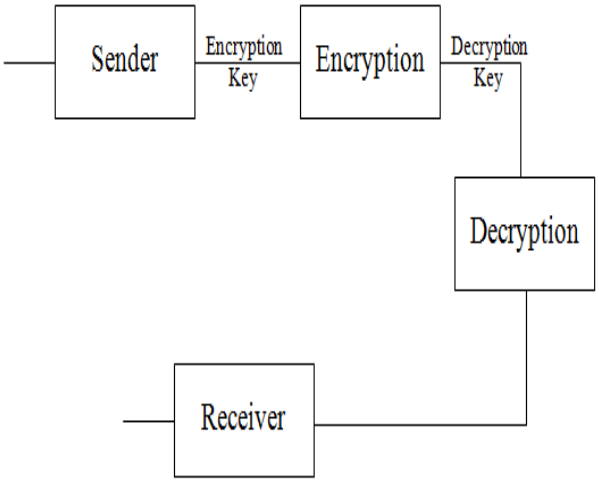

Figure 1: Encryption and Decryption of Data

The above algorithm has the time complexity for transfer of data from one machine to another machine and computed as $O(\log_2 N)$. Let us consider a plain text as POLICY which is implemented in table 1 as shown below:

Table 1: Encryption of Plain Text POLICY

Sender		Ciphers	Receiver	
Plain Text	**X**	**$Y=2^x$**	**$Z=\log_2 Y$**	**Plain Text**
P	16	65536	16	P
O	15	32768	15	O
L	12	4096	12	L
I	9	512	9	I
C	3	8	3	C
Y	25	33554432	25	Y

Table 2: Table 1: Encryption of Plain Text POLICY

Sender		Ciphers	Receiver	
Plan Text	**X**	**$Y=2^x$**	**$Z=\log_2 Y$**	**Plan Text**
I	9	521	9	I
N	14	16384	14	N
S	19	524288	19	S
U	21	2097152	21	U
R	18	262144	18	R
A	1	2	1	A
N	14	16384	14	N
C	3	8	3	C
E	5	32	5	E

In the above example, we take a simple text and finds the alphabetical values in the standard alphabets and find their

corresponding values. These corresponding values converted in the ciphers through $Y=2^X$ the value of this objective function is send as cipher code of information or in other words as encryption key and at receiving end the encryption key generate by $Z = \log_2 Y$. The value of this function is equal to the corresponding value of standard alphabets. Finally one can get the original message as shown in above two examples. The UML model is also shown below in figure 2.

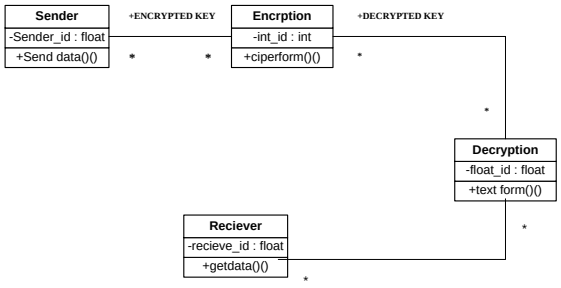

Figure 2: UML Modeling for Encryption and Decryption:

4. CONCLUSIONS

Sending data from sender to receiver is called data communication. Now a day's, security is the interesting area of researchers in data communication as well as other concern. Although there are more research has been done related to OLAP data cube which provide the edges of business concerns so this area need some techniques for providing security. In the proposed paper a mathematical procedure which performs the encryption of data and a key that is used as cipher a message and decipher it back to decode the sending message. Since the proposed technique is based on totally mathematical and it provides the more secure mechanism to hide the sending information. Through the proposed algorithm (SEAOLAP) data cube generates the mathematically bits of stream that are flow in air as signal form for communication. Therefore finally we can say that the proposed algorithm is more secure and reliable. As a future work this type of algorithm can be used in other techniques of data mining.

REFERENCES

[1] Nidhi Singhal, J.P.S.Raina "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", *International Journal of Computer Trends and Technology*- July to Aug Issue 2011.

[2] H. Brown, Considerations in Implementing A Database Management System Encryption Security Solution, A Research Report presented to The Department of Computer Science at the University of Cape Town, 2003.

[3] G. Davida, D. L. Wells, and J. B. Kam, "A database encryption system with subkeys," *ACM Transactions on Database Systems*, vol. 6, no. 2, pp. 312–328, 1981.

[4] H. Hacig¨um¨us, B. Iyer, and S. Mehrotra, "Providing database as a service," in *Proceedings of ICDE*, pp. 29–38, 2002.

[5] J. He and M. Wang, "Cryptography and relational database management system," *IDEAS*, pp. 273–284, 2001.

[6] Oracle, *Oracle9i Database Security for eBusiness*, An Oracle White Paper, June 2001.

[7] Richa Kumari Sharma, S.R.Biradar, B.P.Singh, "Shared Architecture forEncryption/Decryption of AES" International Journal of Computer Applications, Volume 69– No.18, pp-1-6, May 2013.

[8] Balajee Maram,K Lakshmana Rao, Y Ramesh Kumar, " Encryption and Decryption Algorithm using 2-D Matrices" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, pp-352-356, ISSN: 2277 128X, April 2013.

[9] Ayesha Khan, Parul Bhanarkar, Pragati Patil, " RSA Encryption Technique based on Geo Location" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, pp-352-356, ISSN: 2277 128X, April 2013.

[10] Priti V. Bhagat, Kaustubh S. Satpute, Vikas R. Palekar, "Reverse Encryption Algorithm: A Technique for Encryption &Decryption" International Journal of Latest Trends in Engineering and Technology, Vol. 2 Issue 1, pp-99-95, January 2013.

[11] Sunita Bhati, Anita Bhati, S. K. Sharma, "A New Approach towards Encryption Schemes: Byte – Rotation ncryption Algorithm" Proceedings of the World Congress on Engineering and Computer Science, Vol II, pp-1-4, October 24-26, 2012.

[12] Ravindu Madanayake , Nikila Peiris, Gayan Ranaweera,"Advanced Encryption Algorithm Using Fuzzy Logic" International Conference on Information and Computer Networks, IACSIT Press, Singapore, vol. 27, pp-32-36, 2012.

[13] OMG "Unified Modeling Language Specification", 2010, http://www.omg.org.

[14] Amol Bhosle, Yogadhar Pandey, "Applying Security to Data Using Symmetric Encryption in MANET" International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 1, pp-426-430, January 2013.

[15] Pia Singh, Prof.Karamjeet Singh, "IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM IN MATLAB" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, pp-150-154, July-2013.

[16] Mohini Chaudhari, Dr. Kanak Saxena, "Fast and Secure Data Transmission using Symmetric Encryption and Lossless Compression" International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 2, pp.58 – 63, February 2013.

[17] Rajan.S.Jamgekar, Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA" International Journal of Emerging Science and Engineering (IJESE), Volume-1, Issue-4, pp-11-14, February 2013.

[18] Reza Moradi Rad, Abdolrahman Attar and Reza Ebrahimi Atani, "A Comprehensive Layer Based Encryption Method for Visual Data" International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 6, No. 1, pp-37-48, February, 2013.

[19] Weng-Long Chang,Minyi Guo ; Ho, M.S., "Fast parallel molecular algorithms for DNA-based

computation: factoring integers" NanoBioscience, IEEE Transactions on Volume:4 , Issue: 2 , pp-149 – 163, June 2005.

[20] Meikang Qiu, Wenzhong Gao ; Min Chen ; Jian-Wei Niu ; Lei Zhang, "Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System" Smart Grid, IEEE Transactions, Volume:2 , Issue: 4, pp- 715 – 723, Dec. 2011.

[21] N. Kumar, Y. D. S. Arya, "Rate Controlled Adaptive Resource Coordination Framework for Wireless Aware Multimedia Applications", International Journal of Computer Science and Network Security, pp. 99-105, Vol. 10, No. 12, December 2010.

[22] Narander Kumar, Vishal Verma, Vipin Saxena, "Data Cube Representation for Vehicle Insurance Policy System", International Journal of Computer and their Application. pp. 1-4, Vol. 58, No. 1, November 2012.

[23] Dr. Mukul Chandra Pal, "Data Security And Cryptography Based On DNA Sequencing" International Journal of Computer Applications, pp-1-9, Volume 10, Issue No: 3:, July/August , 2013.

[24] Manpreet Kaur, Rajbir Singh, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing" International Journal of Computer Applications (0975 – 8887) Volume 70– No.18,pp-1-6, May 2013.

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. 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.