Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 01, January -2018

Enhancement of Cloud data security by implementing Group Key segregation

[1]Abinesh.P,[2]Balaji.V,[3]Aswin Kumar.T
[4]Saraswathi.V

[1, 2, 3]*U.G. Student Computer Science and Engineering, S.A. Engineering College, Chennai*
[4] *Assistant Professor, Computer Science and Engineering, S. A. Engineering College, Chennai*

ABSTRACT:- *Online data sharing in cloud across geographical boundaries for multiple file sharing using single group key encryption work follows the online data sharing over the cloud by providing group key encryption for group of data over cloud. The Group key acts as a common encryption and decryption key for specific group of data. This lead to a major security thread leak of group key will lead to unauthorized use of group of data. To overcome group key leak problem the key is subdivided into three or more keys.*

Keywords: *cloudcomputing, encryption, decryption, group key, file sharing.*

I. INTRODUCTION

Implementation of cloud computing has pushed the limits of data sharing capabilities for numerous applications that transcend geographical boundaries and involve millions of users. Governments and corporations today treat data sharing as a vital tool for enhanced productivity. Cloud computing has ability to allow multiple users across the globe share and exchange data with less effort. Though there are many advantages, the cloud is prone to privacy and security attacks these are the major drawbacks that prevents cloud computing to attain wholesome acceptance state as the primary means of data sharing.
The most primary requirements that a user would want in a cloud based data sharing service are Data Confidentiality, User revocation, Scalability and Efficiency, Collision between entities.

II. LITERATURE SURVEY

a. Customizable Elliptic Curve Cryptosystems
For the elliptic curve cryptography systems over the finite field GF(2) hardware designs are produced using the optimal normal basics for the description of numbers. The field multiplier is designed by parallel architecture contains multiple bit serial multiplier, these multiplier numbers are altered to achieve the different execution of tradeoffs in speed, security, and size. To fulfill the user demand, design generator has been developed that will create a customized ECC hardware design. To promote the performance of the design a parametric model for evaluating the number of cycles for generic ECC architecture is developed.

b. Analysis of Fractional Window RecodingMethods and Their Application to
Elliptic Curve Cryptosystems
Elliptic Curve Cryptosystems (ECC) are more relevant for memory limitation devices because of their narrow key size. The elliptic curve scalar multiplication is acommon operation in ECC that is window methods, which strengthen the ability of the binary method by performing some pre computation. The organized methods for window methods are sliding window on NAF (NAF+SW), wNAF, and wMOF. The disadvantage of this theory is only little amount of the numbers with suitable sizes for pre computation tables can be undergone. So, there is mandatory to waste memory because the table is not fitting into the exact accessible storage. In this wNAF design there is a modification that allows to unlimited table sizes, so fractional wNAF (Frac-wNAF) is used. By using Markov theory for the estimation of the average non zero density of the Frac-wNAF can be provided with extensive proof. The fractional wMOF (Frac_wMOF) can be proposed here which has a comparable for all left to right functions in FarcewNAF. Frac-wMOF had inherits the impressive properties of Frac-wNAF. Due to its left-to-right nature, FracwMOF is more desirable because it shorten utilization of the scalar multiplication. Finally, we show that all the properties of past schemes are overhead by with special instances of Frac-wMOF method. For computing elliptic curve scalar multiplication with selected amount of memory a practical demonstration of Frac-wMOF by using on-the-fly algorithm is demonstrated.

c. Pipelined Computation of Scalar Multiplication in Elliptic Curve Cryptosystems

The pipelining scheme has been proposed for implementing the Elliptic Curve Cryptosystems (ECC).The principle operation in ECC in scalar multiplication. It is implemented by a series of point additions and doublings. The key notice of this scheme is to begin a subsequent operation, one need not to wait until the current one exit. While the current operation is still being processed, the next operation can be started. Hence the scalar multiplication operations are performed in pipelined manner. The proposed scheme can be made strong the side channel attacks(SCA). SCA-resistant sequential and parallel methods are equated more preferably with our scheme.

d. A Secure and AuthenticatedKey Management Protocol (SA-KMP) for Vehicular Networks

Public Key infrastructure is known for it's popularity but has it's own drawback. It cannot be used in a Vehicular network. A Secure and Authenticated Key Management Protocol (SA-KMP) is designed in which the entities and their public key are combined together and are sent to each and every vehicle on the road. Using this method, the overhead of certifications are eliminated and it reduces computational costs by making use of symmetric keys. SA_KMP seems to outperform PKI in terms of storage, network latency, key generation time also SA_KMP is more secure against active attack, denial of service, etc...

e. Impossible Differential Fault Analysis on the LED Lightweight Cryptosystem in the Vehicular Ad-Hoc Networks
With VANET's growing as the most widely used technology light weight cryptosystems are used for avoiding attacks. These light-weight cryptosystems LED makes use of 64-bit and 128-bit secret keys which provides security to the RFID and other constraints in the vehicles. But researchers have found fault in the last three rounds of the LED. But unfortunately the secret key can be broken by using the IDFA attack.

f. More on Security of Public-Key Cryptosystems Based on Chebyshev Polynomials
The public key cryptosystems based on the Chebyshev polynomial is proved to be insecure. Issue of computational precision needs to be addressed because of two reasons,One is that any cryptosystem is defined using real numbers and during the transmission of messages, the numbers are curbed to a level of precision. Next issue is that this precision issue makes the system insecure. With general precision settings this algorithm can be broken. Using short vector problem in lattice and linear congruence's, the certain classed of the cryptosystems are proved to be insecure.

g. Nonnegative Matrix Factorization Applied to Nonlinear Speech and Image Cryptosystems
Non-negative Matrix factorization (NMF), used in signal separation and image compression inspired to propose a Non-linear Mixing Model in which strong noise is used for encryption and NMF is used for decryption. The non-invertibilily of the designed multivariable non-linear function and the non-negativity of the matrix that can be inversed from the constructed linear mixing matrix are the major aspects considered for security. This system is more efficient than the Lin's model because multi padding can be used and there are no limitations on the features of the plain text and cipher text. So, more signals can be processed irrespective of their characteristics.

h. Reconfigurable Computing Approach for Tate Pairing Cryptosystems over Binary Fields
Public key cryptosystems are replaced by Tate Pairing Cryptosystems because the latter can be used in multi-party identity key management.

- Cupic elliptic
- Binary elliptic
- Binary hyper elliptic are the schemes that can be used in the computations.

Here, a new FGPA-based architecture is proposed over binary elliptic that can take numbers larger than the proposed architecture with same security which reduces the computational cost and improves the performance of the system.

i. Known-Plaintext Attack to Two Cryptosystems Based on the BB Equation
It suffices four distinct plaintext-cipher text pairs to retrieve the primary and secondary keys for the both symmetric cryptosystems to compute in a feasible way. In equation nX+1=Y (mod p) the values of X and Y are assumed to be surplus in order to avoid vulnerable function and this cannot play a major role in cryptanalysis. This cryptanalysis does not perform any factorization algorithms and it involve in computing a greatest common factors and that should not be greater than a module p. Hence the gcd (u, v) can be computed more efficiently by using the Extended Euclidean Algorithm.

III. CONSOLIDATION TABLE

S.NO	TITLE	DEVICE OR METHOD	IMPROVEMENTS
1	Customizable Elliptic Curve Cryptosystems	Produce hardware designs for elliptic curve cryptography (ECC) systems	A design generator has been developed. fastest reported: for a key size of 270 bits.
2	Analysis of Fractional Window Recoding Methods and Their Application to Elliptic Curve Cryptosystems	Elliptic curve cryptosystems	Develop an on-the-fly algorithm for computing elliptic curve scalar multiplication with a flexibly chosen amount of memory.
3	Pipelined Computation of Scalar Multiplication in Elliptic Curve Cryptosystems	pipelining scheme	proposed scheme cannot be made side channel attacks
4	More on Security of Public-Key Cryptosystems Based on Chebyshev Polynomials	public-key cryptosystem based on Chebyshev polynomials	real numbers and during the transmission of messages, the numbers are curbed to a level of precision
5	Nonnegative Matrix Factorization Applied to Nonlinear Speech and Image Cryptosystems	signal separation and image compression method.	strong noise is used for encryption and NMF is used for decryption
6	Reconfigurable Computing Approach for Tate Pairing Cryptosystems over Binary Fields	Tate-pairing-based cryptosystems	new FPGAbased architecture of the Tate-pairing-based computation over binary fields
7	Known-Plaintext Attack to Two Cryptosystems Based on the BB Equation	symmetric cryptosystem	plaintext-cipher text pairs to retrieve the primary and secondary keys

IV. CONCLUSION

Through this key security system we could be able to achieve a par security standard which sharing data and this will play a major role in futue in the domain of cloud computing in the process of sharing data.

V. Reference

1. Thomas Wollinger, Jan Pelzl," Cantor versus Harley: Optimization and Analysis of Explicit Formulae for Hyperelliptic Curve Cryptosystems", IEEE TRANSACTIONS ON COMPUTERS, VOL. 54, NO. 7, JULY 2005.
2. Pina Bergamo, Paolo D'Arco, Alfredo De Santis, and LjupcoKocarev, " ecurity of Public-Key Cryptosystems Based on Chebyshev Polynomials", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, VOL. 52, NO. 7, JULY 2005.
3. Ray C. C. Cheung, Nicolas Jean-baptisteTelle, Wayne Luk, " Customizable Elliptic Curve Cryptosystems", IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 13, NO. 9, SEPTEMBER 2005.

4. Katja Schmidt-Samoa, Olivier Semay, and Tsuyoshi Takagi, "Analysis of Fractional Window Recoding Methods and Their Application to Elliptic Curve Cryptosystems", IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 1, JANUARY 2006.
5. Pradeep Kumar Mishra, "Pipelined Computation of Scalar Multiplication in Elliptic Curve Cryptosystems (Extended Version)", IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 8, AUGUST 2006.
6. FlorianeAnstett, Gilles Millerioux, and Gérard Bloch, "Chaotic Cryptosystems: Cryptanalysis and Identifiability", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, VOL. 53, NO. 12, DECEMBER 2006.
7. Kai Y. Cheong and Takeshi Koshiba, "More on Security of Public-Key Cryptosystems Based on Chebyshev Polynomials", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS, VOL. 54, NO. 9, SEPTEMBER 2007.
8. ShengliXie, Senior Member, IEEE, Zuyuan Yang, and Yuli Fu," Nonnegative Matrix Factorization Applied to Nonlinear Speech and Image Cryptosystems", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, VOL. 55, NO. 8, SEPTEMBER 2008.
9. G. Alvarez, L. Hernández Encinas, and J. Muñoz Masqué, "Known-Plaintext Attack to Two Cryptosystems Based on the BB Equation", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS, VOL. 55, NO. 5, MAY 2008.
10. Chang Shu, Soonhak Kwon, and Kris Gaj, "Reconfigurable Computing Approach for Tate Pairing Cryptosystems over Binary Fields", IEEE TRANSACTIONS ON COMPUTERS, VOL. 58, NO. 8, SEPTEMBER 2009.
11. Chen-Hsing Wang, Chieh-Lin Chuang, and Cheng-Wen Wu, "An Efficient Multimode Multiplier Supporting AES and Fundamental Operations of Public-Key Cryptosystems", IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 18, NO. 4, APRIL 2010.
12. Tim Gurneys, VadimLyubashevsky, and Thomas P€oppelmann, "Lattice-Based Signatures: Optimization and Implementation on Reconfigurable Hardware", IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 7, JULY 2015.
13. Michael Backes, Niklas Grimm, and Aniket Kate, "Data Lineage in Malicious Environments", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 13, NO. 2, MARCH/APRIL 2016.
14. Cai Li, Jiankun Hu, Josef Pieprzyk, and Willy Susilo, "A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 6, JUNE 2015.
15. Wei Li, Wenwen Zhang, DawuGu, Yanqin Cao, Zhi Tao, Zhihong Zhou, Ya Liu, and Zhiqiang Liu, "Impossible Differential Fault Analysis on the LED Lightweight Cryptosystem in the Vehicular Ad-Hoc Networks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 13, NO. 1, JANUARY/FEBRUARY 2016.
16. Hengchuan Tan, Maode Ma, HoudaLabiod, AymenBoudguiga, Jun Zhang, "A Secure and Authenticated Key Management Protocol (SA-KMP) for Vehicular Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 65, NO. 12, DECEMBER 2016.

