International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 11, November-2021

Cloud Data security based on Fuzzy Intrusion Detection system with Elliptic Curve Cryptography (ECC) using Non-Adjacent Form (NAF) Algorithm

Dr. S. Revathi
Researcher
Tamilnadu, India

Abstract:- **To secure massive amount of data ranging from highly confidential business, customer data, financial and to fairly unimportant information in cloud environment, either internally or by third parties we are in need of cloud data protection. This research paper focused on developing a new fuzzy Intrusion Detection System to handles large flow of data packets in network, analyze them and generate reports by integrating knowledge and behavior analysis to detect intrusions. In addition, to enhance the security of the data stored in cloud, Elliptic Curve Cryptography (ECC) using Non-Adjacent Form (NAF) Algorithm is used as encryption techniques to secure data in end-to-end transmission. It increases the confidentiality of the data stored in cloud. So, this paper clarifies how the data is been protected from attackers and a model of algorithm shows how data is encrypted/decrypted. Performance of this proposed system is evaluated with various sizes of text files, on the basis of encryption/decryption processing time and memory. The cloud security levels have also been analyzed and compared with other existing encryption techniques.**

Keywords- Cloud Security, Intrusion Detection System, Fuzzy Logic, Elliptic Curve Cryptography (ECC) and Non-Adjacent Form (NAF).

I. INTRODUCTION

For users, data confidentiality is one of the most prevalent topics in the field of cloud storage. Data stored in a remote server, where the user has no actual control over it and they cannot be able to monitor the behavior of the cloud service provider [1]. The external intruders, or internal service providers, are likely to have a threat and break the confidentiality of the data. The availability of the data is also essential to cloud service provider [2]. The data in cloud storage may imposed to machine failure, network failure, unauthorized access or to any internal invasion leads to Denial of Service (DOS) or Distributed Denial of Service (DDOS) attack to cloud service provider [11]. This paper prosed an Intrusion Detection system as a strong defensive mechanism to secure cloud data [3]. IDS are used to monitor network activities for detecting known or unknown attacks. The main objective of IDS is to generate alarm if any suspicious activity happens.

The proposed system identify break in attempt from unauthorized user. The Cloud security involves various security methods to protect data from unauthorized access or modification [4]. Data encryption is one of the most important factors for improving cloud security, preventing data and tampering data. The data encryption algorithms are broadly classified into two categories a) asymmetrical encryption algorithm (Public- Key-Cryptography) [5]. and b) symmetrical encryption algorithm (Private-Key-Cryptography) [6]. The symmetrical encryption algorithms are RC2, RC4, RC5, DES, 3DES, IDEA, Blowfish and AES. Asymmetric key encryption algorithms are RSA, Robin, ElGamal and Elliptic Curve Cryptography.

This paper proposed a new security mechanism to cloud storage data using intrusion detection system which incorporates Elliptic Curve Cryptography (ECC) for data security and Fuzzy rule generation for attack detection. In ECC, data encryption and decryption are carried out using Elliptical curve arithmetic mechanism, which based on point multiplication that is performed using repeated point addition and point doubling. In addition, Non-Adjacent Form (NAF) Algorithm is used to implement scalar multiplication can speed up encryption process of elliptic curve. The ECC-NAF achieves higher performance level in encryption. The proposed system is used to secure data center and cloud service provider being compromised by the attacker. The proposed result can be deployed in Platform as a Services (PaaS) cloud networking system. Cloud Sim (version 3.1) used for simulation to evaluate rules and to detect intrusion.

II. RELATED WORK

Now-a- days cloud service provider needs to handle multiple requests from the users and need to process them simultaneously, which makes the processing time high and may lead to data and packet delay or corrupt. The cloud storage system improves the data efficiency but not the data security. In [7] author proposed Intrusion detection system at cloud middleware layer. In cloud environment traditional Network IDS are not suitable, since it cannot detect encrypted node communication, also host based IDS are not able to find hidden attack trail. This architecture of IDS include node to access control policies in middleware, The service to facilitates communication through middleware,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 11, November-2021

and event audit monitor to capture network data, to analyzes which rule/policy is attacked. Finally, the storage holds both the behavioral and knowledge-based database. The author tested the IDS prototype by sending the audit data to IDS service core and analyze for attack. The proposed system improves performance satisfaction in real time cloud environment. Though they have not deliberated the security policies compliance check for cloud service provider and their reporting procedures to cloud users.

In [8], Ahmed Patel et.al., describe various IDPSs and alarm management techniques by using machine learning classification and evaluate them to detect and prevent intrusions in Cloud. The results shows that the proposed CIDPS (Cloud Based Intrusion Detection and Prevention System) improves performance with the help of four important parameters like Autonomic computing, fuzzy theory, Ontology and Risk management of the IDPS and cloud computing systems.

Revathi, Malathi [9] described cloud data security based on intrusion detection by generation various fuzzy rules to detect alarm. Initially the data stored in cloud environment will be send to IDS system where numerous fuzzy rules is been generated to check for normal or abnormal data. If the data is from any unauthorized network, the system generate alert to system admin and protect cloud storage from attackers. In addition, once the data is been secured and stored to enhance the confidentiality AES encryption techniques with Differential Fault analysis (DFA) is used to investigate ciphers and extract keys by generating side channel attack as a possession of the attacker. The system improves security and confidentiality of the data stored in cloud.

In [10] author proposed an encryption technique based on Elliptic curve cryptography, to protect information or resource container in the web that are exposed to url. ECC is one of the small key sized and fast computation cryptographic model that consumes less power, memory and bandwidth. The author focused on ECC encryption/decryption techniques to improve confidentiality, integrity and authentication of the data stored. In ECC author used Elliptical curve arithmetic mechanism based on point multiplication that is performed using repeated point addition and point doubling. The author proposed alternative efficient method for point multiplication is binary form or NAF (Non-Adjacent Form). The computation performance with NAF ensures better optimization than the binary form of scalar multiplication.

Mohammad Alkhatib [12] Proposed ECC for Binary Edward and Edward curves using Non adjacent Form (NAF) as encryption process to perform scaler multiplication. This proposed contribution is used in minimizing the time delay via reducing the number of point addition operations performed during scaler multiplication. In addition, Homogenous projective coordinates were used to avoid time consuming-modular inversion operation. The design is implemented parallelly to accelerate ECC computations and achieve the highest performance level.

III. PROPOSED SYSTEM ARCHITECTURE

Data security in cloud environment has been a key point to researcher. Some are focusing on generating better encryption techniques to secure data confidentiality in cloud. The researchers focused on using either asymmetric or symmetric algorithm or a third-party audit to analyze data to ensure with a better encryption and further some are focusing on remote data integrity [13]. This proposed work is to preserve the Cloud storage environment from attackers using IDS security models obtainable with Fuzzy Logic rule generation for Cloud Computing. Further to secure the stored data Elliptic Curve Cryptography (ECC) is used for encryption based on scalar multiplication with point addition and doubling. To increase the performance of scalar multiplication, Non-Adjacent Form (NAF) Algorithm has been used in ECC. The proposed work has been used on CloudSim (version 3.0) and can be deployed on any cloud environment.

With the rapid flow of data been transmitted to cloud storage environment, may lead to dropping of data packets and also host been compromised by an offending attack. In such situation, the proposed system used a network-based IDS with fuzzy rule generation to monitor alerts to cloud service provider for mis-configuration and intrusion attacks in the system. Further the improve data confidentiality in cloud ECC-NAF encryption techniques is used. Fig 1 shows the flow of proposed system.

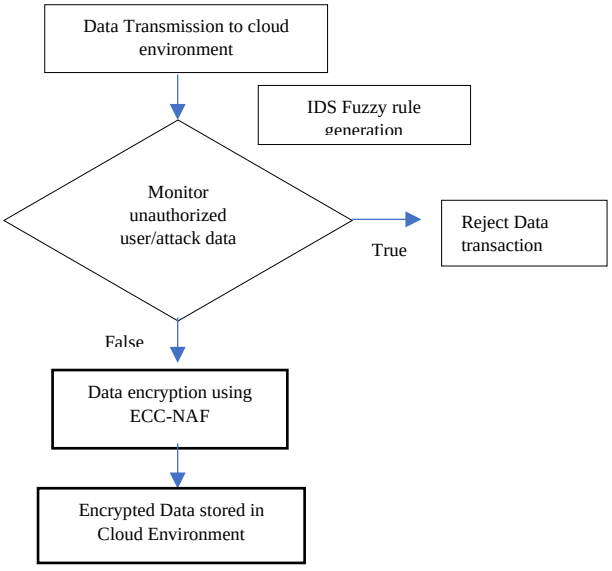

Fig. 1. Proposed workflow

IV. PROPOSED METHODOLOGY

A. *Fuzzy Rule Generation*

Fuzzy system is used for modelling uncertainty of natural language and constructing flexible pattern based on rule-based system that can be structed based on prior

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 11, November-2021

knowledge. Fuzzy system is based on fuzzy logic which provides a computational framework for manipulating and reasoning imprecise knowledge [14]. Fuzzy logic increases robustness and learning adaptability of the intrusion detection system. Popular methods used for fuzzy rule generation are decision trees, association rules, Artificial Neural Networks and evolutionary computation. It is mainly used to separate the normality and abnormality of the connection records in the detection process [15].

Fuzzy Logic and has been proven to be a powerful tool for decision-making and for handling imprecise and noisy data. The central value of a fuzzy system is defined by the truth value of certain linguistic notions and membership values that lie within the range of [0, 1].In Intrusion detection, the security itself includes fuzziness and membership values that lie within the range of [0, 1] The degree of membership of an object takes values between 0 and 1, where 0 means normal data and 1 represent abnormal. The use of fuzziness in representing these numerical attributes helps to smooth the unexpected separation between the normality and abnormality of the data and provides a degree of measure for both scenarios [14].

In this research work, our proposed experimental setup shows the fuzzy rule generation for intrusion detection. Suppose the Parameters taken for this example are Protocol Type, Service, Source Bytes and Destination Bytes.

If(protocol = "tcp")
If(service = "ftp")
If(Source >= 512 && Source <=550 & destination = 512) Then
Transaction type = "probe"

The following example explains it briefly - after training with a large number of data, a typical classification rule will look like

Rule 1: If((source >= 512 & source <= 550)|source = 4096 & ((destination > 2048 & destination < 4096) | destination = 512))

This is an example and some rules are very rarefied as far as understanding them is concerned because the proposed method gives complete freedom to the computer to generate rules to identify/classify an attack.

B. Elliptic Curve Cryptography

ECC was proposed by Miller and Koblitz as a reliable and efficient public-key cryptosystem. ECC uses Discrete logarithm problem for elliptic curve to develop security in cryptographic algorithm. ECC encrypts a message by converting it into a point on elliptic curve, then applying the scaler multiplication operation on that point to yield another point laying on the elliptic curve. The point obtained after the scaler multiplication represents the encrypted message, which can be converted into a ciphertext as well [16].

The researcher focused on using ECC asymmetric ciphers properties with different security applications and its proves that ECC achieves high level of security with smaller key size than other algorithms. It shows that ECC can perform security operations such as encryption and decryption with high performance level or speed and, consuming less resources especially in hardware implementations [17].

Basically, ECC performs modular arithmetic operation over finite fields such as binary field (2m) or prime field GF(p). Encryption is based on scalar multiplication. The two basic scalar operations are point doubling and point addition to obtain cipher text [17]. The computation form for Scalar multiplication is Q= kp where p and Q are the elliptic curve points and k is an integer. This is achieved by repeated point addition and doubling operations. To calculate the above, integer k is represented as $k=k_{n-1},2^{n-1}+k_{n-2}2^{n-2} + \ldots + k_1+k_0$ where $k_{n-1}=1$ and $k_i \epsilon\{0,1\}$, $i = 0,1,2_{n-1}$. This method is called binary method [19] which scan the bits of k either from left-to-right or right-to-left. Below algorithm shows the computation of binary method kp.

Algorithm1: Binary method for scalar multiplication

Binary representation of k and point P
Output : Q = kp
Q=p
For i = n-1 to 0 do
Q = 2Q (Doubling)
If $k_i = 1$ then
Q = Q + p (Addition)
Return Q

The length of k depends on the cost of multiplication and the number of 1s. The number of non-zero digits is called the Hamming Weight of scalar. Average, binary method requires (n-1) doublings and (n-1)/2 additions. For each bit 1, we need to perform Elliptic curve doubling ECDBL and Elliptic curve addition ECADD, if the bit is 0, we need only ECDBL operation. The speed of scalar multiplication or hamming weight will improve based on the reduced number of 1s [18].

C. Non-Adjacent Form (NAF) on ECC

The NAF properties are used in various algorithms, particularly in cryptography for reducing number of multiplications needed for performing exponentiation by squaring depends on Zero bits. If an exponent digit value is 1 its shows as multiplication by the base and if its digit value is -1 its reciprocal. In Scale multiplication Point addition and point doubling are high-level computations for ECC. Each point doubling and addition includes a number of modular multiplications, modular division, and modular addition operations. The modular division operation is the most time-consuming operation since it requires finding the multiplicative inverse [12]. unlike usual implementations

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 11, November-2021

using the Binary method, which assumes that point addition happens half times compared to point doubling, the NAF algorithm's implementation performs point addition one third times compared to point doubling operation. This represents a considerable improvement since it reduces the time consumed by the scaler multiplication operation, and thus the encryption process [20].

Algorithm 2: ECC scalar multiplication using NAF method

Pre-computation Stage:
Input : point P and width d
Output : $P_i = i_P$; i = 1….2^{w-1} -1
P1 = P
X = ECDBL(P1)
For i = 3 to 2^{d-1} - 1, step 2 do
P_i = ECADD(X, Pi-2)
Return P_i;
Evaluation Stage:
Input : point P , k (k is an integer)
wNAF = *skn|skn-1|...|sk0* of *d*
Output : dP
X = 0
for i = n to X do
X = ECDBL(X)
if ki > 0 then
X = ECADD(X, P_{ki})
else if k*i* < 0 then
X = ECADD(X, $-P_{|kj|}$)
return X

NAF is computed from right-to-left least significant bit. So, we need to compute and store the NAF representation of the multiplier before starting scalar multiplication.

V. PROPOSED ALGORITHM

The proposed algorithm passes two stages, initial fuzzy rule generation to monitor abnormal activity and the second part as to secure the stored data in cloud environment based on ECC_NAF encryption method.

Algorithm 3: Proposed Algorithm

1. If T->P to be send from user to CSE. (Where T= data/text to be send, p= No of packets to be send, CSE= Cloud Service Provider)
2. For each T->P, CSE will check P based on FIDS.
3. If FIDS will match (where FIDS= Stored IDS Fuzzy rules to monitor abnormalities of data) detect attack for T->P and identify types of attack.
4. Generate alarm
5. end
6. else
7. For each T->P,
8. Encrypt T->P based on ECC_NAF and send from CSE->DC (Where DC=Data Storage)
9. end

The Proposed ECC_ NAF algorithm performs scaler multiplication, for encryption process which minimize time delay based on point addition and doubling. Further the implementation achieves high performance level in ECC computation

VI. PERFORMANCE EVALUATION

This section focused on performance evaluation of the proposed IDS based cloud environment. Its shows how the proposed system handles data packets and the time measurement to detect attack based on encryption /decryption. Additionally, Cloud security measure has also been analyzed and compared with other existing encryption algorithms. Below table1 shows various input file size used for storage.

Table1: Data File

File name	File size in KB
Data1.doc	1024
Data2.doc	2048
Data3.doc	3072
Data4.doc	4096
Data5.doc	5120

The proposed ECC_NAF is been compared with various Advanced Encryption standard AES algorithm and with AES with Differential Fault Analysis DFA (AES_DFA) [9]. Below table II and fig 2 shows encryption time for different methods measured in milli seconds.

Table II: Encryption time analysis in milli seconds

File Size in MB	AES	AES_DFA	ECC_NAF
1	4226	3113	2933
2	6709	5603	4927
3	9765	8685	7728
4	12897	11634	10448
5	15786	14627	13237

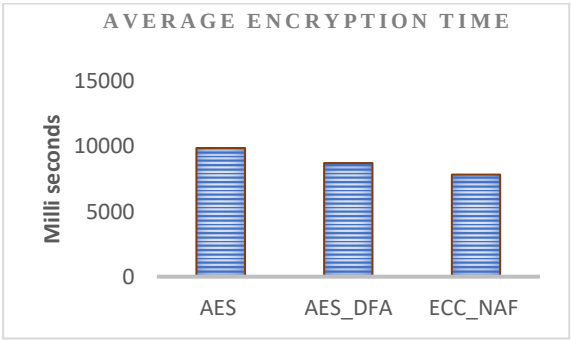

Fig. 2. Average Encryption time

Table III and fig 3 depicts various decryption time analysis with different encryption techniques and compared with proposed method.

Table III: Decryption time analysis in milliseconds

File Size in MB	AES	AES_DFA	ECC_NAF
1	4114	3131	2832
2	6675	5586	4995
3	9671	8717	7722
4	12890	11634	10599
5	15980	14697	13146

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 11, November-2021

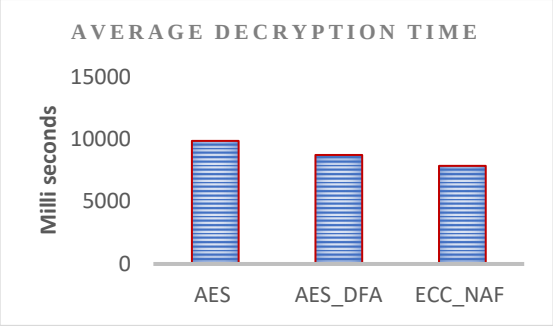

Fig. 3. Average Decryption time

Memory usage analysis for various data size is been shown in table IV and fig 4.

Table IV: Memory usage analysis in bytes

File Size in MB	AES	AES_DFA	ECC_NAF
1	7821	6421	6623
2	8150	7053	7146
3	11449	10541	10860
4	15516	14056	14317
5	18372	17327	17930

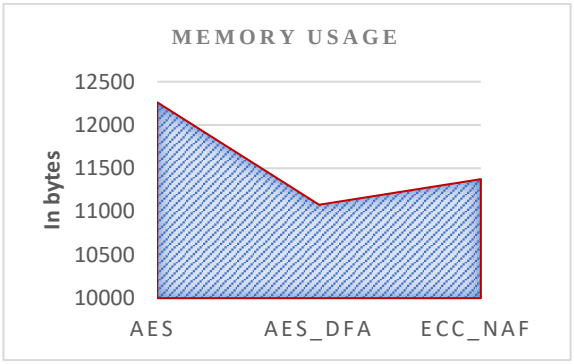

Fig. 4. Average memory usage

In fig 4. The average memory usage for ECC_NAF is more due to its scalar multiplication than AES_DFA. Table V and fig 5 shows cloud environment security level based on fuzzy intrusion detection system (FIDS) and compared with existing encryption techniques.

Table V: Security level in %

Methods	Security level in %
AES	77.1
AES_DFA	87.6
ECC_NAF	90.5

Fig. 5. Security level

VII. CONCLUSION

Cloud environment provides flexible computing resource to its end users and allow to store data, which may lead to security issues. This paper proposed security measures in two different modes. Initially it secures by monitoring and protecting the cloud environment from unauthorized users/ attackers by using a proposed fuzzy based intrusion detection system. FIDS traces attackers more efficiently and protect environments significantly. In addition, to protect the stored data in cloud this paper prosed and tested with new encryption techniques by using ECC along with NAF to increase scalar multiplication time and protect data. The system performances clearly shows that ECC_NAF provides better security and encryption level than existing system. The proposed system also reduces false alarm rate raised by IDS and achieves 90.5%of security level and prevents cloud environment in cost effective manner.

REFERENCES

[1] Preeti Mishraa, Emmanuel S. Pillia, Vijay Varadharajanb, Udaya Tupakulab, “Intrusion detection techniques in cloud environment: A survey”, Journal of Network and Computer Applications, Volume 77, pp. 18-47, 1 January 2017.

[2] Sun Guozi, Dong Yu, Li Yun. “Data access control of cloud storage based on CP-ABE algorithm”, [J]. Journal of communication. 2011 (07).

[3] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, “A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International Conference on Parallel Processing Workshops, 2010.

[4] Huang Ruwei, Gui Lin, Yu Si, Zhuang Wei. “Cloud environment in support of the privacy protection can be calculated encryption method”, [J]. Journal of the computer. 2011 (12).

[5] Nor Badrul Anuar, Hasimi Sallehudin, Abdullah Gani, Omar Zakari, "Identifying false alarm for network intrusion detection system using hybrid data mining and decision tree", Malaysian Journal of Computer Science, Vol. 21(2), 2008 and On Dependable and Secure Computing, Vol. 10, No. 4, July/August 2013.

[6] Ayushi, 2010 "A Symmetric Key Cryptographic Algorithm”, International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15.

[7] Kleber, schulter, “Intrusion Detection for Grid and Cloud Computing”, IEEE Journal: IT Professional, 19 July 2010.

[8] Ahmed Patel, MonaTaghavi, KavehBakhtiyari, JoaquimCelestinoJunior,"An intrusion detection and prevention system in cloud computing: A systematic review", Journal of Network and Computer Applications & 2012.

[9] S. Revathi, A. Malathi, “Cloud Security: Adoption Of Differential Fault analysis On Aes Encryption Algorithm For Data Transmission Based Fuzzy Intrusion Detection System”, International Conference on Science and Innovative Engineering (ICSIE) held in Los Angles, USA on 20th -21st September 2017.

[10] R. Menaka, R. S. D. Wahida Banu, “A Non-Adjacent Form (NAF) Based ECC for Scalar Multiplication that Assure Computation Reduction on Outsourcing”, International conference on Computer Networks, Big data and IoT, ICCBI 2018: Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2018) pp. 319-326.

[11] Rongzhi Wang, “Research on data security technology based on cloud storage”, 13th Global Congress on Manufacturing and Management, GCMM 2016, Procedia Engineering 174 (2017) pp. 1340 – 1355.

[12] Mohammad Alkhatib, “Improved ECC Performance Using NAF Algorithm for Binary Edward and Edward Elliptic Curves”, IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.6, June 2019.

[13] M. Sudha, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography," Advances in Computer Science and its Applications, pp. 32-37, 2012.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 11, November-2021

[14] S. Revathi & A. Malathi, "Network intrusion detection based on fuzzy logic", International Journal of Computer Applications, Volume 1, Issue 4, pp. 143-149, February 2014.
[15] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.
[16] N. Koblitz, "Elliptic curve cryptosystem", Mathematics of Computation, Vol. 48, pp. 203-209, 1987.
[17] V. Miller, "Uses of elliptic curves in cryptography", Lecture Notes in Computer Science, Vol. 218, pp. 417-426, 1986.
[18] Wissam Zaki Mizyad Al-Humadi, "Cryptography In Cloud Computing For Data Security And Network Security", Solid State Technology Volume: 63 Issue: 4 Publication Year: 2020
[19] Takagi, T., Jr, D., Yen, S. and Wu, B., "Radix-r non-adjacent form and its application to pairing-based cryptosystem", IEICE. Trans. Fundam., E89-A(1), pp. 115-122, 2006.
[20] E. Karthikeyan, "Survey of Elliptic Curve Scalar Multiplication Algorithms", Int. J. Advanced Networking and Applications, Volume:04 Issue:02 pp. 1581-1590, 2012.