International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 2

ISSN: 2454-4248
360 – 365

Implementation of Optimized Efficient Elliptic Curve Public Key Encryption for Side Channel Attacks

Allwin D[#1], G Suganthi[#2]
[#1]Department of Computer Science, National College, Thiruvananthapuram -9, Kerala
allwin_d@yahoo.com, allwindb@gmail.com
[#2]Department of Computer Science, Women's Christian College, Nagercoil-1
dr_suganthi_wcc@yahoo.co.in

Abstract: Cloud computing offers both services that provide resources over the Internet and economic benefits for using these resources. As Cloud services turn out to be more common place, recent works have revealed vulnerabilities connected to cloud systems. Cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. In particular, cloud paradigm advances a danger of information leakage over virtual machine through side-channels. Not at all like conventional computing, the cloud infrastructure supporting a Cloud situation permits commonly doubting customer's concurrent access to the underlying hardware, which leads to a side-channel assault. The target of this paper is to explore potential security issues related to side channel attacks and proposed an Encryption concept against side channel attacks. The proposed work introduces the Data Encryption with Optimized Efficient Elliptic Curve Public Key Encryption (EECPKE).

Keywords: *Cloud, Data Encryption, Side Channel Attacks, Virtual Machine*

*****

I. INTRODUCTION

The side channel attack is one of the common attacks in cloud computing here attackers utilize a malicious virtual machine to retrieve data from the cloud. The existing side channel attacker detection models were affected in terms of detecting accuracy and latency. As the attacker is no longer required to increase unlawful, or generally confined access to the victim's hardware, this basically sidesteps the first, and best safeguard against such attacks. Since a side-channel requires the misuse of a particular bit of hardware, every solution should likewise be adjusted particularly for that hardware channel. This permits us to group side-channel assaults and protections in view of the hardware medium they misuse. The CPU cache is a piece of hardware that is frequently used and deals with sensitive data. This makes it one of the most well-known targets for use in a side-channel attacks as it can all the more effortlessly be utilized to remove helpful information at a high rate. An attack made over this channel is called to as a cache based side-channel attack. Cloud computing is turning out to be more well known, however the main worry of technologists for the Cloud is security [1].

II. WAYS TO ATTACK IN CLOUD

Security concerns related with cloud computing fall into two general classifications: security issues confronted by cloud suppliers (associations giving programming, stage, or framework as-an administration by means of the cloud) and security issues confronted by their clients (organizations or associations who have applications or store information on the cloud). The duty is shared, nonetheless. The supplier must guarantee that their foundation is secure and that their customers' information and applications are ensured, while the client must take measures to sustain their application and utilize solid passwords and validation measures. At the point when an association chooses to store information or host applications on the general population cloud, it loses its capacity to have physical access to the servers facilitating its data. Accordingly, conceivably touchy information is at hazard from insider assaults. As per a current Cloud Security Alliance Report, insider assaults are the 6th greatest risk in cloud computing. Therefore, Cloud Service suppliers must guarantee that careful personal investigations are led for workers who have physical access to the servers in the server farm.

CPU cache based side-channel attacks are right now accepted to be the most unsafe, among side-channel attacks. As of late, there have been numerous distributions about Cloud-particular vulnerabilities and endeavors, particularly the utilization of side-channels to sidestep the virtualization innovation utilized as a part of Cloud frameworks [2]. Among different endeavors, they have as of late been utilized to concentrate private keys in a Cloud domain and yield high information leakage. The greatest attack comes from cache based attacks. Along these lines, the extent of this thesis is constrained to side-channel attacks. In response of these attacks, there have been publication works to moderate suchcircumstances. While advantageous, these arrangements require the customer utilizing them to modify their own software to work with their innovation, or the basic hardware. From understanding the Cloud, we trust that this restriction is both harmful to the client, and superfluous.

 ISSN: 2454-4248
360 – 365

III. SIDE CHANNEL ATTACKS

A channel is a way for conveying data in a computing framework. A side channel is a channel whose essential utilize is not data exchange. Regularly, the presence of such channels is unintended by outline. Side channels have gotten extensive consideration with regards to multi-user operating system, where processes can communicate by means of examples in utilizing, or getting locks on, shared resources, for example, disk space, memory, and processor time. Exploiting side channels normally requires the cooperation of a sending and a receiving process.

Side-channel attacks are anything but difficult to-actualize while effective assaults against cryptographic executions and their objectives go from primitives, conventions, modules, and gadgets to even frameworks. These assaults represent a genuine risk to the security of cryptographic modules. In outcome, cryptographic usage must be assessed for their resistivity against such assaults and the consolidation of various countermeasures must be considered.

IV. DATA ENCRYPTION WITH OPTIMIZED EFFICIENT ELLIPTIC CURVE PUBLIC KEY ENCRYPTION (EECPKE)

The encryption technique is based on Elliptic curve model and converted the public key encryption with the original random hash function into a secure encryption technique as secure over the chosen-cipher text attack. The variables and the steps involved in the EECPKE algorithm is given and explained as follows.

Variables

In this section the variables associated with the EECPKE algorithm is given in the table 1.

Table 1 Parameters for encryption

Parameter	Representation
Symmetric key	κ
Symmetric key Length	κ_{Len}
Plaintext(VM Data)	ρ
Cipher text	c
Length of plaintext	ρ_{Len}

From the table 1, it is to be noted that $\kappa_{Len} = \rho_{Len}$, i.e., the length of the symmetric key and the plaintext (message) will have equal length always since the encryption is performed as a bit-wise operation and this can be understood in the following sections.

Key generation

In this algorithm, the data owner generates key pairs as follows: the data owner chose the two large primes and calculates $N = ab$. Next computes c and d using extended Euclidian algorithm where $ac + bd = 1$. Then public key is $PK = \{N\}$ and private key is $PR = \{a, b, c, d\}$. The process of key generation is illustrated in Algorithm 1.

Algorithm 1. Key Generation

1 Select two large random primes a, b

2 Calculate $N = ab$

3 Compute c & d using Euclidian algorithm
Where $ac + bd = 1$

4 Public Key $PK = \{N\}$ and Private Key $PR = \{a, b, c, d\}$

Randomly Optimized Encryption

The encryption algorithm for EPPKE is represented as E and the input for the algorithm are the plaintext ρ, public key p_κ and the symmetric encryption technique È = $\kappa \oplus \lambda . \rho$ (here $\lambda = [0,1]$ is the random parameter) whereas the output is the cipher text set as given by $c = (c_1, c_2, c_3)$. The process of the encryption technique is illustrated as follows.

- Pick $r \in \{0,1\}^{r_{Len}}$ also $R \in \{0,1\}^{R_{Len}}$ and calculate the symmetric key κ as $G(R)$.
- Calculate $c_1 = g^R h^r \bmod n$, $c_2 =$ È (ρ) and $c_3 = H(c_1, R, \rho)$

Normally in EPPKE three different cipher texts are generated and among them two are $(c_1 \& c_3)$ generated with random parameters and to enhance more security to the cipher text c_2 we have included a random parameter denoted as λ varies from $0:1$ and with that parameter N different number of cipher texts are generated as $c_2 = \{c_2^1, c_2^2, c_2^3, ...c_2^N\}$. From this N number of cipher texts, the best one is obtained with the help of an optimization technique called Covariance Matrix Adaptation Evolution Strategies (CMA-ES) with constraint to the certain parameters.

Random Optimization with Covariance Matrix Adaptation Evolution Strategies (CMA-ES)

The optimization of the cipher texts generated randomly through the above encryption process is done with the aid of the optimization technique called Covariance Matrix Adaptation Evolution Strategies (CMA-ES) which is similar to some basic concepts involved in Genetic algorithm (GA) (Recombination) as well as Particle swarm optimization (PSO) (Population Based). But the advantage of the CMA-ES optimization is that global convergence is achieved in a rapid manner also in GA the history is exploited based on two individuals but here the same thing is done from the weighted average of the group. CMA-ES is the recently developed evolution based optimization and commonly applied to the problem of electromagnetic field. Since its performance is better than GA and PSO algorithm in the convergence speed the optimization of cipher texts can also

 ISSN: 2454-4248
360 – 365

be performed in an efficient manner. The randomly generated cipher texts are optimized with constraint to the parameters called Encryption Quality, correlation coefficient of the cipher texts and differential attack. The definitions and calculation of these parameters, the objective function formulation and the optimization of the cipher texts are clearly illustrated as follows.

i) Encryption Quality

The Encryption Quality is denoted as Q_E and this is calculated for measuring the quality of Bitmap images encryption [3] and here we have modified that calculation for the cipher texts from the plain texts. Then, Q_E for the generated cipher texts is calculated as mentioned below.

- Measure the deviation between the plaintext and the cipher text in how many places they are differing and this is calculated using the following equation (1).

$$d = |\rho - c_2^n|, \; n = 1,2,.....N \qquad (1)$$

- Compute the average value of bits deviation as given in equation (2).

$$\bar{d} = \frac{1}{\rho_{Len}}(d) \qquad (2)$$

- Calculate Encryption Quality Q_E as in equation (3).

$$Q_E = |d - \bar{d}| \qquad (3)$$

This is the first objective of our optimization technique and our aim is to maximize the Encryption Quality and hence the first part of objective function is given as in equation (4).

$$f_1 = \max(Q_E) \qquad (4)$$

ii) Correlation coefficient

The correlation coefficient can be denoted as $r_{\rho c_2^n}$ and this is also one of the parameter used for measuring the correlation between pixels of the encrypted and original image [4] and similarly the correlation between the cipher text and the plain text is calculated and the calculation is given as follows.

- Calculate the mean of both ρ and c_2^n using the equations (5) and (6) given below

$$E(\rho) = \frac{1}{\rho_{Len}} \sum_{i=1}^{\rho_{Len}} \rho_i \qquad (5)$$

$$E(c_2^n) = \frac{1}{\rho_{Len}} \sum_{i=1}^{\rho_{Len}} c_{2\,i}^n \qquad (6)$$

- Measure covariance between ρ and c_2^n using equation (7) as given below.

$$\text{cov}(\rho, c_2^n) = E\left[\left(\rho - E(\rho)\right)\left(c_2^n - E\left(c_2^n\right)\right)\right] \qquad (7)$$

- Then the standard deviations of ρ and c_2^n is calculated using the equations (8) and (9) as given below.

$$std(\rho) = \frac{1}{\rho_{Len}} \sum_{i=1}^{\rho_{Len}} (\rho_i - E(\rho))^2 \qquad (8)$$

$$std(c_2^n) = \frac{1}{\rho_{Len}} \sum_{i=1}^{\rho_{Len}} (c_{2\,i}^n - E(c_2^n))^2 \qquad (9)$$

- Finally $r_{\rho c_2^n}$ is calculated using equation (8) as given below.

$$r_{\rho c_2^n} = \frac{\text{cov}(\rho, c_2^n)}{\sqrt{std(\rho)}\sqrt{std(c_2^n)}} \qquad (10)$$

It is to be noted that depending on the value of $r_{\rho c_2^n}$, the relationship between ρ and c_2^n is decided and for the encryption should be a successful one the relation should be minimum. The value of $r_{\rho c_2^n}$ and the relationship between the original and encrypted texts is given by the following condition in (11).

$$r_{\rho c_2^n} = \begin{cases} > 0, & \text{Strong positive relationship } \rho \text{ and } c_2^n \\ 0, & \text{No relationship } \rho \text{ and } c_2^n \\ < 0, & \text{Strong negative relationship between } \rho \text{ and } c_2^n \end{cases}$$

(11)

As seen from the condition (11) the objective is that $r_{\rho c_2^n}$ should be less than or equal to zero and the second part of the objective function is given as in equation (12).

$$f_2 = \min(r_{\rho c_2^n}) \qquad (12)$$

Then the third objective function called Differential Attack is formulated as given below.

iii) Side Channel attack

Side Channel Attack is the one in which the attacker will try to observe the change in the encrypted data by modifying some bit values in the original data from the VM [5]. There are two measures are used to detect the impact of the single bit value on the whole encrypted image and this also suits for our proposed framework where we analyze the impact of single bit change in the plaintext to that of the cipher text. The measures are (a) Information Entropy factor and (b) Avalanche Effect (AE) and the calculation of these measures are given in equations (13) and (14).

 ISSN: 2454-4248
360 – 365

$$H(m) = -\sum\{0 \le i \le n-1\} p(m_i) \log_2 p(m_i) \quad (13)$$

Where $p(m_i)$ represents probability of m_i.

$$AE = \frac{Ham\min g\ Dis\tan ce}{File\ Size} \quad (14)$$

The measures given in equations (13) and (14) should also be maximum to avoid the Differential Attack and thus the final part of our objective function is formulated as given in equation (15).

$$f_3 = \max(H(m)) + \max(AE) \quad 15)$$

The overall objective function of the proposed method and the optimization of the best cipher text is given in the next section.

iv) Objective function Formulation and cipher text optimization

The formation of the objective function of our proposed framework is thus given by combining the equations given in (4), (12) and (15) and the overall objective function f is given in the equation (16).

$$\left.\begin{aligned} f &= f_1 + f_2 + f_3 \\ f &= \max(Q_E) + \min(r_{\rho c_2^n}) + \max(H(m)) + \max(AE) \end{aligned}\right\} \quad (16)$$

Based on the objective function given in equation (16) the optimization of the cipher text is performed with the help of CMA-ES.

Decryption

After successfully encrypting ρ with randomly optimized EPPKE using CMA-ES that cipher text set is decrypted in the reverse manner at the receiver side and this is illustrated as follows. The input for the Decryption phase D , is the cipher text set $c = (c_1, c_{2opt}, c_3)$ and the secret key s_κ and the output become either the original plaintext or null string based on secret key.

- Calculate $c_p = c_1^{p-1} \bmod p^2$,

  $R' = \frac{L(c_p)}{L(g_p)} \bmod p$ where $L = x \to \frac{x-1}{p}$ for $x = 1 \bmod p$

- Calculate $K' = G(R')$ as well as $m' = D_{K'}(c_{2opt}) = K' \oplus c_{2opt}$
- Check whether the following condition is satisfied

$$c_3 = H(c_1, R', m')$$

If the above condition is satisfied means the output will be the m´as the decrypted text or produce null string

V. RELATED WORK

In 2013, Vijay Varadharajan and UdayaTupakula proposed a novel trust improved security display for cloud benefits that identifies and avoid security assaults in cloud foundations utilizing trusted authentication methods.They consider a cloud engineering where distinctive administrations are facilitated on virtualized frameworks on the cloud by different cloud clients (multi-occupants). They consider assailant display and different assault situations for such facilitated benefits in the cloud. The trust upgraded security show empowers the cloud specialist organization to guarantee certain security properties of the occupant virtual machines and administrations running on them. These properties are then used to distinguish and minimize assaults between the cloud inhabitants running virtual machines on the framework and its clients as well as increment the confirmation of the occupant virtual machine exchanges. On the off chance that there is a variety in the conduct of the occupant virtual machine from the ensured properties, the model permits them to progressively separate the occupant virtual machine or even end the pernicious administrations on a fine granular premise, depicts the outline and execution of the proposed display and talks about how it manages the distinctive assault situations and additionally demonstrate that the model is useful for the cloud specialist co-ops, cloud clients running occupant virtual machines and in addition the clients utilizing the administrations gave by these occupant virtual machines[6].

F.X. Standaert and C. Archambeau proposed [7] three vital inquiries in this regard. First,compare the viability of these two side-channels. Selecting naturally the significant time tests in side-channel spillage follows is a critical issue in the use of layout assaults and it more often than not depends on heuristics and indicate how established measurable devices, for example, Central Component Analysis and Fisher Linear Discriminant Analysis can be utilized for effectively preprocessing the spillage follows.

OnurAcıiçmez and Cetin Kaya Ko proposed the method for proficient follow driven store assaults on a generally utilized execution of the AES cryptosystem, likewise assess the cost of the proposed assaults in detail under the supposition of a quiet situation, build up a precise scientific model that can use in the fetched examination of the assaults. They utilize two unique measurements, particularly, the expected number of fundamental follows and the cost of the examination stage, for the cost assessment purposes. Each of these measurements speaks to the cost of an alternate period of the assault [8].

In 2009,Moti Yung et al. proposed [9] this work makes a step in this bearing and proposes a structure for the investigation of cryptographic usage that incorporates a hypothetical model and an application strategy. The model depends on generally acknowledged speculations about side-channels that calculations offer ascent to. It permits measuring the impact of for all intents and purposes significant spillage capacities with a mix of data theoretic and security measurements, measuring the nature of an execution and the quality of an enemy, individually. From a hypothetical perspective, they illustrate formal associations between these measurements and talk about their instinctive significance. From a viable perspective, the model infers a bound together procedure for the examination of side-channel key recuperation assaults. The proposed

 ISSN: 2454-4248
360 – 365

arrangement permits disposing of the greater part of the subjective parameters that were restricting past specific and regularly specially appointed methodologies in the assessment of physically detectable gadgets.

Michael Backes1 and Boris K proposed the approach is based on a measure of the mystery data that an assailant can extricate from a framework from a given number of side-channel estimations, give a calculation to figure this measure, and utilize it to dissect the resistance of equipment usage of cryptographic calculations with regard to power and timing assaults[10].

VI. RESULTS AND ANALYSIS

Encryption time

The Encryption Quality Q_E is calculated for the different file sizes and used here to depict the quality of our encryption technique. The results of Q_E are presented in the following figure 1 with different file sizes for proposed work.

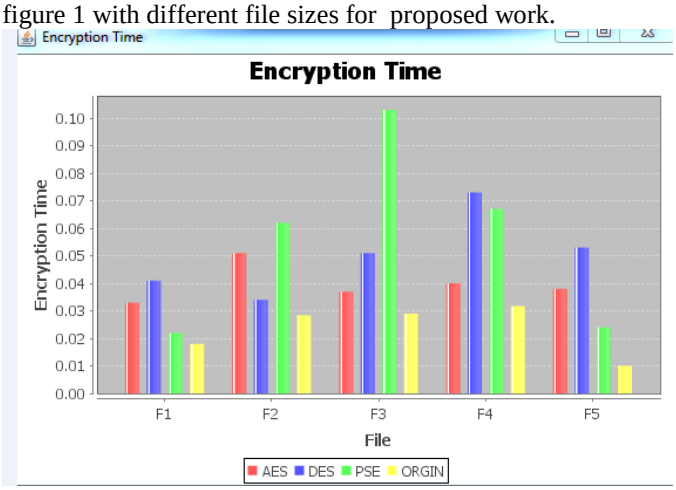

Fig 1. Encryption Time

Decryption time

The below graph indicates the time required to decrypt the data by the different algorithms with different files as shown in fig 2.

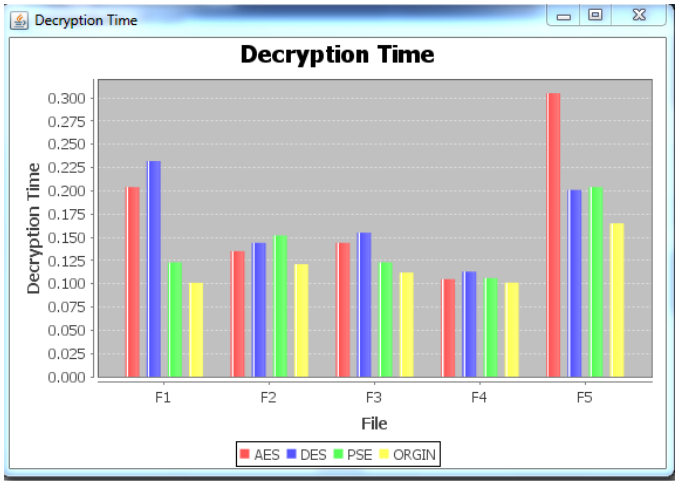

Fig 2. Decryption time

Correlation Co-efficient

The next performance measure is the Correlation Coefficient Factor, which evaluates the correlation between the plain text and cipher-texts produced randomly. The results of CC are presented with different file sizes given in figure 3.

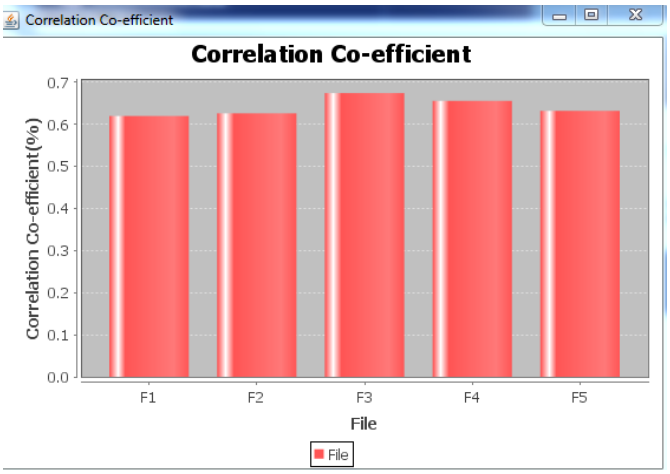

Fig 3.Correlation Co-efficient

VII. CONCLUSION

Using side-channel attack, it can be very easy to gain secret information from a device so it is good idea to provide security against side channel attack in cloud computing using randomly encryption decryption algorithm. The proposed models give better results when compared to the conventional methods for preventing side channel attacks. Like with side-channel attacks, the Cloud gives a domain particularly powerless against numerous other side-channel attacks. There emerges an awesome trouble in tending to them in light of the fact that, as medium specific attacks, they regularly require a better solution. As such, every possible channel will require additionally work to build up a solution based to its specific vulnerabilities.

VIII. REFERENCES

[1]. IDC. Enterprise it in the cloud computing era, 2008.

[2]. Shuo Chen, Rui Wang, XiaoFeng Wang, and Kehuan Zhang. Side-channel leaks in web applications: A reality today, a challenge tomorrow. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, SP '10, pages 191–206, Washington, DC, USA, 2010. IEEE Computer Society

[3]. Michael Backes and Boris Kopf, Formally Bounding the Side-Channel Leakage in Unknown-Message Attacks, pp 517-532,volume 5283,springer 2009

[4]. OnurAcıicmez and Werner Schindler,A Major Vulnerability in RSA Implementations due to MicroArchitectural Analysis Threatiacr, 2007.

[5]. ZHAO Xin-jie, WANG Tao, ZHENG Yuan-yuan,Cache Timing Attacks on Camellia Block Cipher National Natural Science Foundation of China (Grant No. 60772082)

[6]. Vijay Varadharajan and UdayaTupakula,Counteracting security attacks in virtual machines in the cloud using

ISSN: 2454-4248
360 – 365

property based attestation, Journal of Network and Computer Applications 40 (2014) 31–45.

[7]. F.-X. Standaert and C. Archambeau,Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages, University College London International Workshop on Cryptographic Hardware and Embedded Systems.

[8]. OnurAcıicmez and C¸ etin Kaya Koc,Trace-Driven Cache Attacks on AES, Oregon State University,springer 2006.

[9]. Francois-Xavier Standaert, Tal G. Malkin andMoti Yung, A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks,Version 3.0, volume 5479, springer 2009.

[10]. Michael Backes and Boris Kopf, Formally Bounding the Side-Channel Leakage in Unknown-Message Attacks, pp 517-532,volume 5283,springer 2009