10.48047/jocaaa.2024.33.05.50

Designing Cloud-Native Intrusion Detection Systems with API Transaction Intelligence

Navneet Kumar Tyagi Senior Software Developer, Finance of America navneettyagi.research @gmail.com	Abhishek Verma abhishekverma.techie1 @gmail.com Director Digital Operations, Anthem Inc, Atlanta, GA	Rohit Tewari rohittewari.fintech@ gmail.com Unysis Sr Java Lead/ Architect	Amit Prasad Associate Consultant, Tata Consultancy Services Ltd amitp.research@g mail.com"	Harvendra Singh Principal Software Engineer, Publix Super Markets Inc harvendra.research @gmail.com

Abstract

With the exponential rise of cloud-native applications, safeguarding API-driven communications has become a critical priority. Modern cloud platforms expose numerous endpoints, often becoming primary targets for adversarial activities such as injection attacks, privilege escalation, and data exfiltration. Traditional intrusion detection systems (IDS) struggle to adapt to the dynamic and decentralized nature of cloud-native environments. This research introduces a novel design for a Cloud-Native Intrusion Detection System (CN-IDS) that leverages API transaction intelligence to detect malicious behaviors in real time. The proposed CN-IDS integrates contextual API usage patterns, behavioral baselining, and anomaly detection powered by lightweight machine learning models. Unlike conventional signature-based methods, our system continuously learns from evolving API traffic, identifying threats even in zero-day or obfuscated scenarios. Special focus is placed on analyzing transaction sequences, authentication anomalies, and rate-based deviations across microservices. The system is designed to be natively deployed within Kubernetes and serverless environments, ensuring scalability and low latency. Experimental evaluation in hybrid cloud testbeds demonstrates that the proposed model significantly outperforms existing IDS approaches in both detection accuracy and response time, while maintaining minimal overhead. By embedding API transaction intelligence, the CN-IDS fortifies cloud-native infrastructures against a broad spectrum of threats without disrupting normal operations..

Keywords: Cloud Environment, API, Cloud Pailier, Rapid Cloud Pailier, Safety and Intruder.

Introduction

The cloud computing is a booming platform that makes use of wide range of technology for disseminating on demand services like storage, networks, applications and servers with the help of internet [1,2]. It is possible because of various technologies offered by the cloud service suppliers comprising minimal costs, potent computations, improved service flexibility and

10.48047/jocaaa.2024.33.05.50

scalability. However, the focus is on safeguarding confidential information which is still a great dispute faced by cloud computing thereby limiting its global access.

The computations over the encoded information could be regarded as a best possible solution to win the disputes faced by the environment [3]. The scholars have suggested a fresh encoding scheme termed as homomorphic encoding that intends to provide a third party with the possibility to perform operations over the encoded information. This homomorphic feature makes the scheme of great use in terms of safeguarding confidentiality for example consider a voting system and digital healthcare system [4].

It rooted the existence of several homomorphic encoding schemes. The scheme is usually categorized into two classes as partial and comprehensive homomorphic encoding. The scheme of the initial class offers one feature of homomorphism in a very limited manner [5]. The comprehensive homomorphic scheme provides various homomorphic features in parallel [6].

The sub – contracted encoded information of homomorphic scheme could be saved for long time instances with the use of same key over the cloud environment and the cloud users frequently makes use of these cloud services through resource restricted devices. The schemes require being encouraged in terms of security levels and time of execution.

The Pailier's scheme for confidentiality [7] is employed effectively over the cloud environment so that the design intention is based on the cloud Pailier. The cloud pailier encoding scheme attempts to resolve an exception of the Pailier's scheme alongside aids the inclusive homomorphism in terms of integers and opposes increased safety threats. The scheme is safe under the double trapdoor presumptions and the rigidity for factoring immense and merged integers along with hard decision based amalgamated redundant presumptions.

The cloud Pailier scheme is solely for the creating modulus m = xy formed from two distinct primes and the creation of an integer i $\in p_{n^2}$ fulfilling $i^{\lambda} \equiv 1 (\text{mod m})$, here λ = lcm (x – 1, y – 1). The modulus m represents the assessment key and (m, i, λ) symbolizes the private key. The encoding scheme is encoded and decoded based on the private key as in the Pailier scheme [8]. The assessment key is employed by the third party to carry out inclusive homomorphism over the encoded information.

The intention is to recommend a rapid alternate to the cloud Pailier encoding scheme for fastening its decoding. The rapid alternative safeguards the form of cloud Pailier encoding and

10.48047/jocaaa.2024.33.05.50

uses the Chinese remainder for decoding. The designed difference aids the inclusive homomorphism thereby offers an immense rapidity in decoding over the cloud Pailier scheme while preserving the same level of safety.

Related Works

Due to the development of homomorphic encoding [9] innumerable homomorphic based schemes aid the inclusive homomorphism. Two homomorphis scheme aids the inclusive homomorphism over the integers. The encoding schemes are safe under the issue of factoring immense and complex integers along with the issue of decision with complex redundancies.

The design of rapid homomorphic scheme attempts to encode the simple information that is encrypted as either 0 or 1 but for decoding it averts noise. The technique is safe by the Euclidean Lattices and the time for execution is based on the sequence of operations being performed [10,11]. The Gentry's encoding scheme is not useful of several applications as it encodes information bit length and the execution time is improved along with the levels of safety.

The design of a novel homomorphism termed as Digital Gentry's Homomorphism works on integers that attempts to encode simple information as either 0 or 1 which is safe based on the precisely large common advisor problem. However the public of the Digital Gentry's Homomorphism prevails over $\Omega(\lambda^{10})$ which is practically immense [8] [9].

The Grouped Gentry's Homomorphism aids encoding and homomorpism process over the bit vectors of the information. The designed scheme is safe in terms of semantics and encodes bits as one cipher text.

The Pailier's cryptosystem is enhanced in terms of confidentiality to work flawlessly over the cloud computing environment [2] [5]. The designed encoding technique resolves the issues with the Pailietr's scheme aiding the inclusive homorphism over the integers and withstands more threats in terms of safety. The cloud Pailier scheme accomplishes safety using double trapdoor considerations as the hardness of factoring huge complex integers and the hard decision based complex and redundant perceptions.

The sub – contracted encoded information based on the homomorphic scheme can be stored for elongated time over the cloud computing environment as the users of the cloud holds the access to the services offered by the cloud platform through the resource restricted devices as

10.48047/jocaaa.2024.33.05.50

the technique requires to the promoted in terms of safety levels but also on execution time to work flawlessly.

The intention is to focus on the cloud Pailier encoding scheme [7]. The decoding scheme is very much boosted for effective working without compromising the confidentiality levels of the cloud computing platforms. A varied scheme is suggested which preserves the same set of cloud Pailier encoding and makes use of the Chinese residue for decoding.

The designed scheme is very identical for its usage along with the Chinese residue to gear up the usual RSA scheme [2] [5] [8] and the decoding of the cloud RSA [10] alternatives such as the MultiPrime Cloud RSA [7]. The re-equalized cloud RSA [9] and the Multi-power cloud RSA [8] [9]. For all the schemes the decoding exponent is of the order modulus 'm'. For gaining rapid decoding, the decoding is carried out as modulo of each of the prime factors of 'm' and the partial decoding are aggregated based on the Chinese residue to acquire the actual plaintext.

Preliminaries

The preliminary holds some theorems that are quite essential for the forthcoming sections.

Hypothesis 1 (Chinese Residue)

Let x_1 and x_2 be two positive integers that are in combination co – prime and let y_1 and y_2 be two integers which resembles,

$$\begin{cases} a \equiv y_1 (\mathrm{mod}\, x_1) \\ a \equiv y_2 (\mathrm{mod}\, x_2) \end{cases} (1)$$

comprises an exclusive solution

$a = y_2 + ((y_1 - y_2).\ x_2\ \mathrm{Inv}\ (\mathrm{mod}\ x_1))$ (2)

where, $x_2\ \mathrm{Inv} \equiv x_2^{-1} (\mathrm{mod}\ x_2)$ (2)

Hypothesis 2 (Euler's Theorem)

Let z, m $\in$ P in a way that gcd(z,m) = 1, then

$$z^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)\ (3)$$

10.48047/jocaaa.2024.33.05.50

Here, $\phi(m) = x_1^{\alpha_1 - 1}(x_1 - 1).....,x_k^{\alpha_k - 1}(x_k - 1)$ in a way that x_1,.....,x_k are distinctive primes.

Hypothesis 3 (Binomial Theorem)

Let a $\in$ P and p, q $\in$ Q, then

$$(p+q)^x = \sum_{k=0}^{x} \binom{x}{k} (p)^{x-k} (b)^k \quad (4)$$

where, $\binom{x}{k} = \frac{x!}{k!(x-k)!}$

Hypothesis 4

Let the set $X_n = \{a < m^2\}$, $a \equiv 1 \pmod m$, for $m \in P$, $\forall_a \in X_n$, then the function is defined as:

$$S(a) = \frac{k-1}{m} \quad (5)$$

Modelled Homomorphic Scheme

The intention is to recommend a rapid variation of the cloud Pailier encoding scheme [9] [10]. The intention is to offer an essential routines for cloud Pailier's variation. The effectiveness of these variations assesses their level of safety.

Routines

The routine for creation of keys, encoding, assessment and decoding of cloud Pailier's variation is presented. The rapid difference is concerned on the creation of modulus m = xy created from two voluminous and discrete primes (x, y) and upon the creation of integet p > 1 in X_{n2}, X_n = {0, 1,.....,m-1} fulfilling $p^{\lambda} \equiv 1 \pmod m$ and gcd (L($p^{\lambda} \pmod{m^2}$), m) = 1, here λ=lcm (x – 1, y – 1) and gcd represents greatest common divisor. The modulus m is public and symbolises the assessment key. The primes x and y along with the integers p and λ remains private and in order to gain access to added decoding and rapidity it is possible to pre – estimate the Chinese residue co – efficient yInv and the values $(L(p^{x-1} \pmod{x^2}))^{-1} \pmod x$ and $(L(p^{y-1} \pmod{y^2}))^{-1} \pmod y$ as it is stored as a part of the private key. The creation process is portrayed in routine 1.

Routine 1: Creation of Keys

10.48047/jocaaa.2024.33.05.50

Input: Two large and discrete primes x and y.

Result: An assessment key a_k = (m) and a private key k_p = (x, y, p, p_1, p_2, yInv).

Estimate m = xy and λ = lcm (x – 1, y – 1).

Choose an integer $p \in X_{n^2}$ in a way that $p^{\lambda} \equiv 1(\mathrm{mod}\, m)$ and gcd ($L(p^{\lambda} \pmod{m^2})$, m) = 1.

Choose $p_1 = (L(p^{x-1} \pmod{x^2}))^{-1} \pmod{x}$ and $p_2 = (L(p^{y-1} \pmod{y^2}))^{-1} \pmod{y}$.

Choose: yInv $\equiv y^{-1} \pmod{y}$.

Return (m) and (x, y, p, p_1, p_2, yInv).

The difference encodes a message $c \in X_n$ under the private key which safeguards the identical forms of encoding as in cloud Pailier technique. The encoding process is portrayed in routine 2.

Routine 2: Encoding

Input: Private key (x, y, p, p_1, p_2, yInv) and a plain text $c \in X_n$.

Result: $c_t = e(c_t, c)$.

Choose an arbitrary $r \in X_n$ in a way that gcd (r, m) =1.

Estimate $c_t = p^c, r^x \pmod{m^2}$.

Return c_t.

The cloud service provider can perform inclusive homomorphism over the encoded information based on the assessment key. The process of assessment is portrayed in routine 3.

Routine 3: Assessment

Input: An assessment key a_k and cipher texts c_1,....., c_m.

Result: $c_t = A (a_k, c_1.,,,,,,c_m)$.

Estimate

$A (a_k, c_1.,,,,,,c_m) \equiv c_1$ x.....x$(\mathrm{mod}\ m^2)$

10.48047/jocaaa.2024.33.05.50

$\equiv (p^{c1}\ r_1^m)$ x.....x $(p^{cm}\ r_m^c)$ (mod m^2)

$\equiv p^{c1+.....+cm}(r_1$ x.....x $r_m)^m$ (mod m^2)

$\equiv a_k(a_k, c_1+.....+c_m)$

Return A $(a_k, c_1+.....+c_m)$

Here, A is the assessment function.

The rapid cloud Pailier encoding is performed based on the private key by making use of the Chinese residue hypothesis 1.

Routine 4: Decoding

Input: Private key (x, y, p, p_1, p_2, yInv) and the returned cipher text c_t.

Result: $c = c_1+.....+c_m$.

Estimate $c_x \equiv L\ (m^{x-1}$ (mod x^2)) x p_1 (mod x) and $c_y \equiv L\ (m^{y-1}$ (mod y^2)) x p_1 (mod y).

Employ Chinese residue and estimate

$c = c_x + y((c_x - c_y)$ x yInv (mod x)).

Return c.

Accuracy

Here the intention is based on the accuracy of the decoding scheme of the modelled variation. Let m be the resultant of two discrete primes x and y along with $p \in X_{n^2}$ in a way that $p^{\lambda} \equiv 1$ (mod m) and gcd ($L(p^{\lambda}$ (mod m^2)), m) =1 for p > 1.

Let r $\in X_n$ in a way that gcd (r,m) =1.

$r^{m(x-1)} = r^{\phi(x^2)y}$ (6)

$= (r^{\phi(x^2)y})$

$\equiv 1$ (mod x^2) (based on hypothesis 2)

In relation to equation 6,

10.48047/jocaaa.2024.33.05.50

$r^{m(y-i)} \equiv 1(\text{mod}\, y^2)$ (7)

Equation 6 and 7 gets rid of arbitrary integer that is appended based on the encoding process.

Consider that $p^{\lambda} \equiv 1 (\text{mod m})$ (x-1) divides λ and (y-1) divides λ, so

$p^{\lambda} = p^{\alpha(x-1)}$ (for (α>0)) (8)

$\equiv 1$ (mod x) based on hypothesis 2

and

$p^{\lambda} = p^{\beta(x-1)}$ (for (β>0)) (9)

$\equiv 1$ (mod y) based on hypothesis 2

Here, $p^{x-1} \equiv 1$ (mod x) and gain $p^{y-1} \equiv 1$ (mod y) i.e. $p^{x-1} = 1 + p_{k_1,x}$ and $p^{y-1} = 1 + p_{k_2,y}$ for p_{k1}, p_{k2} $\in X^*$. It is possible to estimate $(1+p_{k1})^{cx}$ for $c_x \in X_n$ based on hypothesis 3.

$$(1+p_{k_1})^{c_x} = \sum_{i=0}^{c_x} (c_i^x)(p_{k_1})^i \quad (10)$$

$$= 1 + cp_{k_1} + \sum_{i=2}^{c_x} (c_i^x)(p_{k_1})^i$$

$$\equiv 1 + cp_{k_1} (\text{mod}\, x^2)$$

Likewise,

$(1+p_{k_2})^{c_y} \equiv 1 + cp_{k_2} (\text{mod}\, y^2)$, for $c_x \in X_x$ (11)

Estimate c^{x-1} modulo x^2 and x^{y-1} modulo y^2.

$c^{x-1} \equiv p^{c_x(x-1)} (\text{mod}\, x^2)$ based on eqn. 8

$\equiv 1 + cp_{k_1} (\text{mod}\, x^2)$ based on eqn. 10 (12)

$c^{y-1} \equiv p^{c_y(y-1)} (\text{mod}\, y^2)$ based on eqn. 9

$\equiv 1 + cp_{k_2} (\text{mod}\, y^2)$ based on eqn. 11 (13)

10.48047/jocaaa.2024.33.05.50

gcd ($L(p^{x-1} \pmod{x^2})$, x) = 1 and gcd ($L(p^{y-1} \pmod{y^2})$, y) = 1, as gcd ($L(p^{\lambda} \pmod{m^2})$, m) = 1 and therefore, (($L(p^{x-1} \pmod{x^2})$ and ($L(p^{y-1} \pmod{y^2})$ have their modulo x and y,

$c_x = L(c^{x-1} \pmod{x^2}) \times p_1 \pmod{x}$ and $c_y \equiv L(c^{y-1} \pmod{y^2}) \times p_2 \pmod{y}$ (14)

Effectiveness

Estimation is carried out for the theory based execution time for decrypting the rapid cloud Pailier variation requiring the need of cloud Pailier technique.

The cloud Pailier technique is recalled for recalling the actual message c from a cipher text c_t by estimating,

$$c \equiv \frac{L(c^{\lambda} (\mathrm{mod}\, m^2))}{L(p^{\lambda} (\mathrm{mod}\, m^2))} (\mathrm{mod}\, m), for(\lambda \equiv lcm(x-1, y-1)) \quad (15)$$

For estimating $c^{\lambda} \pmod{m^2}$, $p^{\lambda} \pmod{m^2}$ and $(L(p^{\lambda} \pmod{m^2}))^{-1} \equiv (L(p^{\lambda} \pmod{m}))$ for each of the equation, the technique considers the execution time $\theta(\log(\lambda)\log^2(m))$. For λ to the order of m, the execution time is $\theta(\log^3(m))$.

In the rapid cloud Pailier variation [11-15], the process of decoding requires two exponentiations modulo $(\frac{m^2}{2})$ bit numbers. Hence, the estimation of c^{x-1} requires the execution time $\theta(\log^3(\frac{m}{2}))$. The Chinese residue steps requires insignificant time as estimated to the full exponentiations, where one computes the decoding execution time of the rapid variations that is $\frac{3n^3}{2(\frac{\pi}{2})^3} = 12$ times quicker than of the cloud Pailier scheme.

Assessing Confidentiality

The rapid cloud Pailier variance holds the identical levels of confidentiality of cloud Pailier's scheme. The safeties of the variation are based on double hard issues.

a) The hardness of factoring a complex integer m = xy where x and y are quite discrete. It is simple to estimate m = xy but no polynomial time scheme are termed to factorize the outcomes.

10.48047/jocaaa.2024.33.05.50

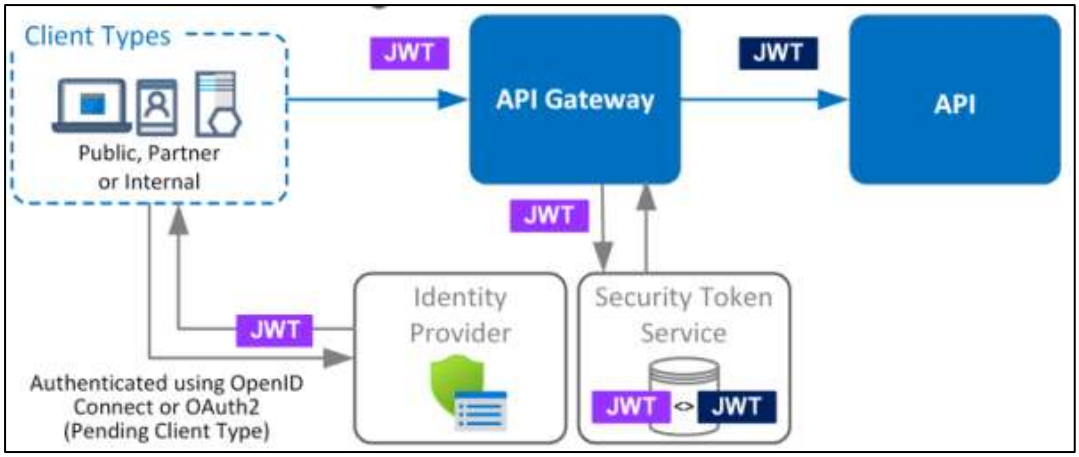

Figure 1: Overall security model

b) The hard decision based complex arbitrary assumptions (HDCAA) provided with the prime factors of the modulus m and an integer X, it is quite complex to decide whether X is a λth residue modulo m^2 or not i.e. whether it prevails within an integer $p \in X_{n2}$ in a way that:

$$X \equiv p^{\lambda} \pmod{m^2} \quad (16)$$

The cloud Pailier variation is choice based and safe based on HDCAA. Hence, the variation is semantically safe. In order to offer an improved level of safety the modulus must contain two secure primes and these primes does not suit within the abilities of the rapid factorization threats namely number field sieve and elliptic curve method.

Results and Discussions

The rapid cloud Pailier variation is planned and estimated against the cloud Pailier technique. The performance evaluation of decoding time is estimated based using Python. The planning is carried out using a smart phone.

The modulus is set to m = xy of balanced and discrete primes and of 1024 bit numbers. The creation of the key pairs is performed based on PARI / GP system. Table 1 symbolizes the needed time in ms for decoding the related encoded information of quantity ranging from 100 to 1000 bits using cloud Pailier scheme and its variations.

Table 1: Performance of Decoding

10.48047/jocaaa.2024.33.05.50

Bit Size of Plain Text	Cloud Pailier (ms)	Cloud Pailier Variations (ms)
100	2100.86	250.33
200	2022.52	242.65
300	2165.52	249.25
400	2099.16	250.45
500	2002.45	246.12
600	1989.32	240.11
700	2011.12	238.45
800	2033.56	238.56
900	2089.23	230.22
1000	2156.32	256.48

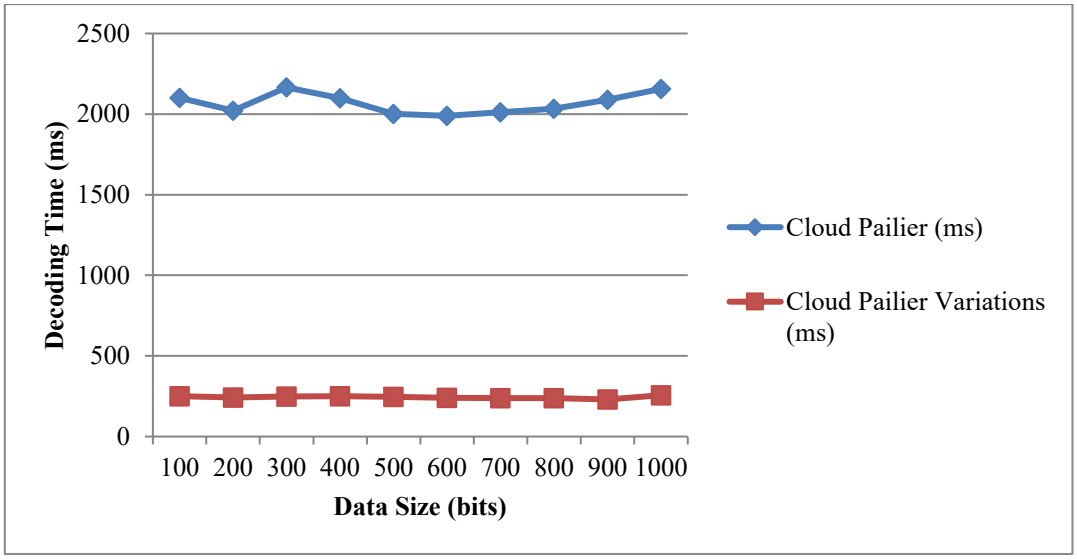

Figure 2: Comparing Decoding Time of Cloud Pailier and its Rapid Variation

The outcomes of the simulation reveal that the cloud Pailier variation gains decoding is increased by a factor of 9 over the cloud Pailier scheme. The Chinese residue scheme (step 2 of routine 4) needs insignificant levels of time as estimated against the comprehensive exponentiation of the cloud Pailier decoding. Fig. 1 reveals that the decoding time of the cloud

10.48047/jocaaa.2024.33.05.50

Pailier scheme and its variation is roughly constant as all the cipher texts are based on the order of m^2.

Conclusion

The intention is to model a rapid variation of the cloud Pailier scheme to speed up the process of decoding. The variation holds the identical form of the cloud Pailier modulus and encoding scheme and makes use of Chinese residue for decoding. It aids the inclusive homomorphism over the integers and it is semantically safe. The outcomes of the simulation reveal that the designed variation gains an immense speed over the cloud Pailier while safeguarding the identical level of safety. The further work is intended on speeding up the cloud Pailier scheme to a suggested level.

References

1. Dr. L. Arockiam,S. Monikandan, ―Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm‖, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Volume 2, Issue 8, ISSN : 2278-1021, August 2013, pp. 3064-3070.
2. Atiq U R Rehman, and M. Hussain, ―Efficient cloud data confidentiality for DaaS‖, International Journal of Advanced Science and Technology, Vol. 35, 2011, pp. 1-10.
3. Yau SS, An HG, ―Confidentiality protection in cloud computing systems‖, International Journal Software Informatics, Vol. 4, Issue 4, 2010, pp. 351-365.
4. ManpreetKaur and Rajbir Singh, ―Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing‖, International Journal of Computer Applications, Vol. 70, Issue 18, 2013, pp. 16-21.
5. Yu S, Wang C, Ren K, Lou W, ―Achieving secure, scalable, and fine-grained data access control in cloud computing‖, In: INFOCOM, 2010 proceedings IEEE, pp. 1–9.
6. Nashaat el-Khameesy, Hossam Abdel Rahman, ―A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems‖, Journal of Emerging Trends in Computing and Information Sciences, Volume 3, Issue 6, 2012, pp. 970-974.
7. V. D. Cunsolo, S. Distefano, A. Puliafito, and M. Scarpa, ―Achieving information security in network computing systems‖, Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC'09.), 2009, pp. 71-77.
8. Hadi, S., Alireza, S., Behnam, B. and Mohammadraze, A., ―Cryptanalysis of 7-Round AES-128‖, International Journal of Computer Application, 10, 2013, pp. 21-29.
9. Preethi, P., Vasudevan, I., Saravanan, S., Prakash, R. K., & Devendhiran, A. (2023, December). Leveraging network vulnerability detection using improved import vector machine and Cuckoo search based Grey Wolf Optimizer. In *2023 1st International Conference on Optimization Techniques for Learning (ICOTL)* (pp. 1-7). IEEE.
10. Alex, B. and Johann, G., ―Cryptanalysis of the Full AES Using GPU-Like Special-Purpose Hardware, Journal Fundamental Informatics—Cryptology in Progress‖, 10th Central European Conference on Cryptology, 10-12, 2010, Vol. 114, pp. 221-237.

10.48047/jocaaa.2024.33.05.50

11. Bernstein, D., Chen, H., Chen, M., Cheng, C., Hsiao, C. and Lange, T., ―The Billion-Mulmod-Per-Second PC‖, In SHARCS ’09: Special-Purpose Hardware for Attacking Cryptographic Systems, Lausanne, 2009, pp. 131-144.
12. Zhao G, Rong C, Li J, Zhang F, Tang Y, ―Trusted data sharing over untrusted cloud storage providers‖, IEEE second international conference cloud computing technology and science (CloudCom) 2010, pp 97–103.
13. Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y, ―Fine-grained data access control systems with user accountability in cloud computing‖, IEEE second international conference on cloud computing technology and science (CloudCom) 2010, pp. 89–96.
14. Goyal V, Pandey O, Sahai A, Waters B, ―Attribute-based encryption for fine-grained access control of encrypted data‖, 13th ACM conference on computer and communications security (CCS ’06) 2006, pp. 89–98.
15. Ammi, M., Adedugbe, O., Alharby, F. M., & Benkhelifa, E. (2022). Leveraging a cloud-native architecture to enable semantic interconnectedness of data for cyber threat intelligence. *Cluster Computing*, *25*(5), 3629-3640.