Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

# Security of AI Based Prediction using Paillier cryptosystem

Brook Hilemriam *[1], Asamene Kelelom [2], Beer Singh[3]

[1,2] College of Engineering and Technology Samara University, Ethiopia.
[3]Seth Vishambhar Nath Institute of Engineering & Technology, Barabanki, UP, INDIA

Email: [1]brookhailemariam@su.edu.et, [2]asamenek@su.edu.et , [3]beersinghtu@gmail.com

*Corresponding author E-mail: brookhailemariam@su.edu.et



## Abstract

This paper demonstrates the practical operation of the Paillier cryptosystem in securing direct retrogression conclusion while conserving data sequestration. A customer- garçon armature is used, where sensitive input data is translated on the customer side using Paillier's cumulative homomorphic encryption and reused on the garçon without revealing the raw values. The translated data is subordinated to a direct retrogression model (with a predefined weight and bias), using homomorphic operations to cipher translated prognostications directly. After decryption, the works corresponded exactly to the expected direct results, thus confirming the correctness of the calculations in the translated space. A performance test carried out on a dataset of 30 numerical values showed an average of the encryption and decryption times of 0.31 seconds and 0.28 seconds respectively. Nevertheless, the performance is quite effective for small to medium-scale datasets. Such a system yields a highly secure sequestration- conserving output for sensitive operations like healthcare analytics or fiscal modelling. The findings indicate that the model keeps computational consistency even when the data is encrypted, thus enabling precise and reliable predictions that do not compromise data security. Also, the simplicity and availability of the perpetration using Python and the PHE library make it a practical choice for real- world deployments. While presently limited to direct models due to the cumulative nature of the Paillier scheme, the approach presents a strong case for extending sequestration- conserving ways to broader classes of machine literacy algorithms. This exploration highlights the eventuality of homomorphic encryption in enabling secure and secure AI systems, especially in scripts where confidentiality is consummate.

***Keywords:*** *Security of AI Models, Paillier Cryptosystem, Linear Regression, Homomorphic Encryption, Artificial Intelligent.*

## 1.0 Introduction

In current years, Artificial Intelligence (AI) and Machine Learning (ML) algorithms have become the necessary tool for different industries, such as healthcare, finance, education, and defense. It has been

Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

noticed that AI applications frequently require a lot of personal data, for example, patient data, finance transactions, user data, to learn from and create accurate predictions about specific parameters. But this learning process has made it a serious concern for privacy and security because improper access to this data has made it vulnerable to breaches, identity theft, and misuse of proprietary information. Additionally, AI models are valuable intellectual property [1] . Displaying model parameters or allowing unrestricted access during diagnosis can result in model inversion attacks, theft of model IP, or adversarial exploitation. To address these concerns, researchers are exploring privacy-preserving machine learning techniques that allow computations to be performed on encrypted data thus protecting both the user's data and the service provider's model. In these days, where artificial intelligence is reshaping our world, security has become a most important concern. Security is not just an essential component of a computer system, it's the lifeblood that guards its functionality, credibility, and trust. Traditional IT security implementations, which involve protecting systems, combating attacks, and strengthening defenses against adversarial red teams, are well-established. However, the rapidly growing field of Artificial Intelligence (AI) introduces fresh challenges that require attention and specialized approaches. These challenges obligate us to escalate our efforts to protect the ever-growing digital ecosystem. Cryptography is concerned with studying how we can protect data, offering security against trespassers. Much of the security depends on cosmopolitan means to obtain pseudorandom mappings that are reversible, allowing both encryption and decryption tasks [2] . The robustness of cryptographic algorithms often banks on publicizing the algorithms for the community to study for feebleness and possible attacks so that when a vulnerability is detected, the algorithm can be updated or patched. This public nature of algorithms also has positive effects concerning mass production, implementation, and deployment; moreover, one important additional aspect that must not be overlooked is trustworthiness: knowing exactly how the algorithm works, or at minimum knowing that one can have access to that information creates trust. Cryptography plays a climacteric role in securing AI models and their data. By taking on various cryptographic techniques, we can ensure the covertness, integrity, and privacy of AI systems. Homomorphic encryption is a promising solution to this issue, as it authorizes computation on encrypted data without requiring decryption. As we move on deeper into the world of AI security, it is important to familiarize ourselves with the particular cryptographic techniques that can be implemented. This particular cryptographic technique is the Paillier cryptosystem, which we will delve into later on in the next sections. There exist numerous homomorphic encryption schemes. However, one particular scheme that stands out is the Paillier cryptosystem because it has particular properties involving addition that makes it capable of performing computation on encrypted data through addition and linear transformation. Therefore, through the Paillier cryptosystem, it is now possible for AI to make predictions on encrypted data to ensure data privacy through/influencing the Paillier cryptosystem. Introduction to the Paillier Cryptosystem is a game-changing development for securing AI models. This advanced cryptographic tool is transforming the way we protect our intelligent systems from threats, now capable of functioning as a strong defense mechanism against threats while AI models can continue to function properly. In this particular application, linear regression is capable of functioning through the Paillier cryptosystem to encrypt predictions on encrypted user data to ensure data privacy [3] .

In this paper, we explore how the Paillier cryptosystem can be applied to secure AI models. It provides contouring of its mathematical foundation, discusses integration strategies with AI models (including linear regression), and evaluates the benefits and limitations in experiential. The focus is to display how homomorphic encryption—especially using Paillier can offer strong security guarantees while using effective AI deployment in privacy-sensitive environments. The table 1 shows the applications of cryptography in AI in terms of security.

Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

**Table. 1:** Applications of Cryptography in AI

| Application | Description | Benefits |
|---|---|---|
| Model Protection | Encrypts AI models to prevent unauthorized access | Preserves intellectual property |
| Data Privacy | Encrypts training data and inputs | Protects sensitive information |
| Secure Inference | Allows computations on encrypted data | Enables privacy-preserving predictions |
| Federated Learning | Enables collaborative learning without data sharing | Preserves data locality and privacy |

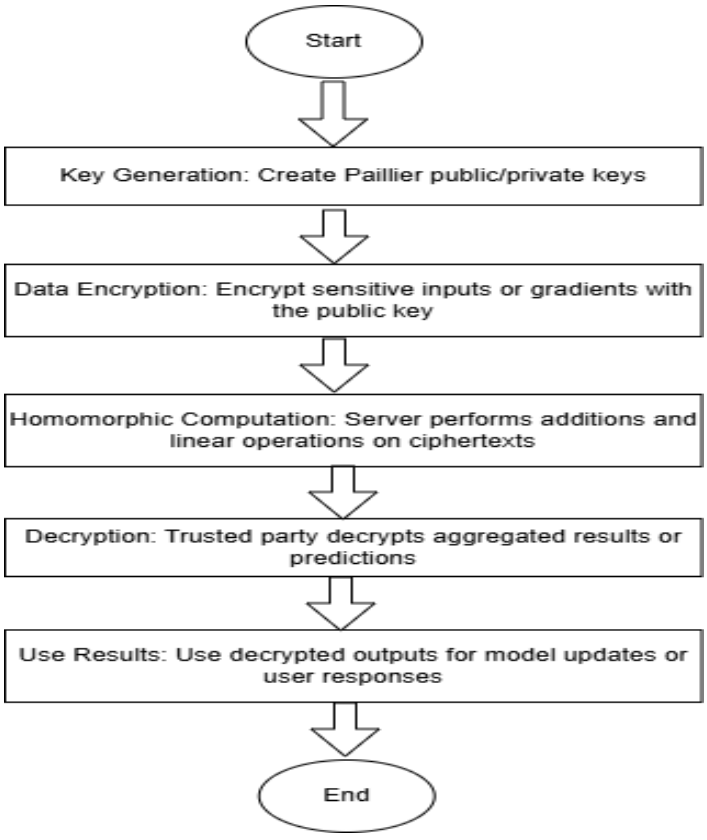



**Fig .1:** Architecture of Security with AI Models

The Fig. 1 represented architecture of security with AI models. Here, a trusted party secretes public and private keys based on large prime numbers. With this scheme, the trusted party encrypts the sensitive input information like model weights in such a way that the encrypted data cannot reveal patterns in relation to the original data. Most importantly, the server carrying out the computation can perform addition operations on these encrypted data without actually having the data. Finally, the result of the encrypted data is returned to the trusted party, and based on the private key, the trusted party can derive the outcome of the computation.

Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

## 2.0 Background

Umpteen research papers have proposed different approaches for AI model sharing, addressing various aspects of security and privacy. Li, T., Sahu,[1] introduces federated learning, a collaborative approach that enables training models across distributed devices without sharing raw data, thereby preserving privacy. It discusses the challenges and potential solutions associated with federated learning. Bonawitz [2] introduces a system design for large-scale federated learning, focusing on addressing challenges related to communication, security, and model aggregation. It discusses the design considerations and the potential impact of federated learning at scale. Due to its large storage facility and high-end computing capability, cloud computing has received great attention as a huge amount of personal multimedia data and computationally expensive tasks can be outsourced to the cloud. Shah et al. [3] proposed a solution for non-integer mean value computation in the homomorphic encrypted domain without any interactive protocol between the client and the service provider. Using the proposed solution, various image processing operations, such as local smoothing filter, un-sharp masking, and histogram equalization, can be performed in the encrypted domain at the cloud server without any privacy concerns. The use of linear support vector regression on private data in cloud computing must consider data privacy. Homomorphic encryption is an approach to address the problem. Sari, A. K. [4] the used a model to predict the motor and total UPDRS (Unified Parkinson's Disease Rating Scale) scores. To assess the performance of the model, the MRSE (Mean Root Square Error) of the prediction on the prediction on encrypted data is exactly the same as that on unencrypted data, which proves that the modification on the operations in linear support vector regression has been done correctly. Altaee [5] present a proposal to secure banking data transmission through the cloud by using partially homomorphic encryption algorithms such as (Paillier and RSA algorithm) that allow performing mathematical operations on encrypted data without needing to decryption. A proxy server will also use for performing re-encryption process to enhance security. Palle and Punitha [6] proposed method is based on recent contributions and focuses on tailoring homomorphic encryption algorithms like Paillier and Fully Homomorphic Encryption (FHE) to specific machine learning tasks. To strike a balance between data utility and privacy, seamless compatibility with preprocessing pipelines is prioritized. Secure model preparation strategies, consolidating cryptographic conventions and secure conglomeration techniques, are crucial in saving the secrecy of delicate data. security of user's data is a very big problem which can be solved using Homomorphic encryption. Kiratsata [7] worked, first the spiderman correlation of the machine learning models developed using encrypted dataset is compared with each other. In which the algorithms used to encrypt dataset are Homomorphic Encryption (HE) based Rivest Shamir Adleman (RSA) and Paillier algorithm. Su and Geng [9] proposed a secure two-party euclidean distance computation (SEDC) scheme under a covert adversarial model based on Paillier encryption. In the scheme, the secure two-party Euclidean distance was computed by using technologies, such as Paillier encryption, and the computation results were verified with each other to ensure that both parties sent real data and had no cheating in the process of parameter interaction. To overcome these constraints numerous authenticated key agreements schemes considered to enhances performances and security. However, high latency and heavy cryptographic operation entails time and bits overheads. Hasan [9] the novel proposed key distribution enables efficiency, security, and data privacy which is emerging notions for the smart metering infrastructures. Gong, B. [10] presents an efficient zero-knowledge argument of knowledge system customized for the Paillier cryptosystem where system enjoys sublinear proof size, low verification cost, and acceptable proof generation effort, while also supporting batch proof generation/verification. Existing works specialized for Paillier cryptosystem feature linear proof size and verification time. Using existing sublinear argument systems for generic statements (e.g., zk-SNARK) results in unaffordable proof generation cost since it involves

Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

translating the relations to be proven into an inhibitive large Boolean or arithmetic encrypted data is then compared with the MRSE of the prediction on unencrypted data. The evaluation shows that the MRSE of circuit over a prime order field. It system does not suffer from these limitations.

## 3.0 Background

## 3.1 Homomorphic encryption

Homomorphic encryption is the turning of data into ciphertext that can be evaluated and worked with as if it were still in its eccentric form. Homomorphic encryption empowered complex mathematical operations to be performed on encrypted data without yielding the encryption. In mathematics, homomorphic mark outs the transformation of one data set into another while preserving relationships between elements in both sets. This term is derived from the Greek words for same structure. Because the data in a homomorphic encryption scheme preserves the same structure, identical mathematical operations will provide equivalent results -- regardless of whether the action is performed on encrypted or decrypted data. Homomorphic encryption differs from typical encryption methods because it entitles mathematical computations to be performed directly on the encrypted data, which can make the handling of user data by third parties safer.

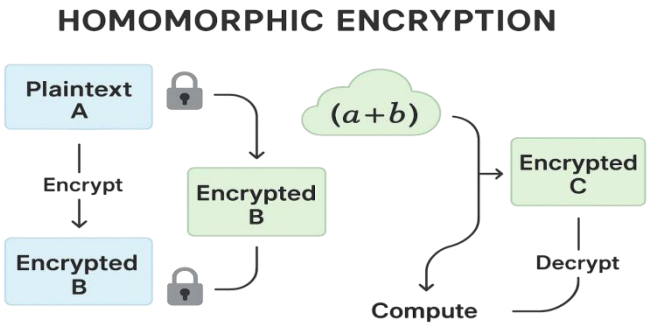



**Figure 2.** Compute encrypted data with homomorphic encryption

Homomorphic encryption is outline to create an encryption algorithm that entitles an infinite number of additions to encrypted data. The Paillier cryptosystem, introduced by Pascal Paillier in 1999, is based on composite degree residual classes and offers semantic security under the Decisional Composite Residuosity Assumption (DCRA) [11]. These encryption scheme enables two fundamental homomorphic properties, the risk one is additive homomorphism, where the product of two ciphertexts results in the encryption of the sum of their plaintexts, and the second is scalar multiplication, where a ciphertext raised to a constant power results in the encryption of the product of the plaintext and the constant. These properties make the Paillier cryptosystem particularly suitable for secure computations in linear models, where the output is a weighted sum of the inputs. Acar, M. (2018) has done a Survey on Homomorphic Encryption Schemes [12]. Saxena and Kumar [15-17] have provided the design of the hybrid architectures involving fuzzy logic, ElGamal mutual authentication, biometric hashing, and hierarchical DNA-Paillier cryptography. This performs better than other approaches regarding security, bandwidth utilization, and encryption speed in insecure networks. There is also the three-tier AES-RSA-ECIES and the AES-Paillier hybrid approach that further improves the security of the data as well as key exchange [18]. There is the Dual phase Hypervisor Controller based on EM clustering and fuzzy time series that provides better results for

Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

DDoS attacks in the cloud as opposed to the IDS system [19].
Homomorphic Encryption schemes can be classified in table 2 as partially, somewhat, or fully homomorphic based on the operations and depth of computation they support.

**Table 2:** Types of homomorphic Encryption

| | **Partially** | **Somewhat** | **Leveled Fully** | **Fully** |
|---|---|---|---|---|
| **Rating** | Simple | Intermediate | Advanced | Most advanced |
| **Computations** | Addition or multiplication | Addition or multiplication | Complex but limited | Complex and unlimited |
| **Use cases** | Sum or product | Basic statistical analysis | AI/ML, MPC | AI/ML, MPC |

## A. Partially Homomorphic Encryption

The simplest type, partially homomorphic encryption, entitles either additions or multiplications to be performed on the encrypted data, but not both. It can compute the product or sum of a dataset. It perform specific operation to be performed on encrypted data without decrypting it,

The Paillier cryptosystem is divided into two partially-homomorphic cryptosystem, the scheme 1 is the basic version of Paillier cryptosystem and the second is highly secure and faster decryption. The security of Paillier cryptosystem is depends on n-th residues in $\mathbb{Z}_{n^2}^*$ and the hardness of integer factorization [13].

### Step 1: key generation

Select any prime numbers p and q.

Compute n=p*q

Compute $\lambda = lcm(p-1, q-1)$

g, with $g \in \mathbb{Z}_{n^2}^*$ and the order of g is a multiple of n.

public key (n,g) and private key $(p, q, \lambda)$

### Step 2: Encryption

plain text m<n

Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

select any random number r<n such that $r \in \mathbb{Z}_n^*$

get the ciphertext $c = g^m r^n \ mod \ n^2$

### Step 3: Decryption

ciphertext $\boldsymbol{c < n^2}$

plaintext m=$\frac{L(c^\lambda \ mod \ n^2)}{L(g^\lambda \ nod \ \ n^2}$ mod n

## Example:

### Key generation

(1) Pick p = 13 and q = 17. (They satisfy the condition.)

(2) Compute n = 221.

(3) Compute λ = 48.

(4) Pick g = 4886.

(5) Compute μ = 159. (It exists.)

### Encryption

Set a = 123.

(1) Pick r = 59.

(2) Compute c = 13250 mod $221^2$ .

### Decryption

Compute $a_{decrypted}$ = 123 mod 221. (The same as a.)

## B. Somewhat Homomorphic Encryption

Homomorphic encryption allows for both addition and multiplication operations to be performed on the encrypted data, although it has some limitations. Especially, the number of operations that can be performed is bounded and the accuracy of the computation may degrade as more operations are performed. This scheme can be useful for simple evaluating functions or performing basic statistical analyses**.**

## C. Leveled Fully Homomorphic Encryption

A more advanced scheme, leveled fully homomorphic encryption can execute an erratic number of computations on encrypted data, as far as it has a pre-defined sequence of computations to be

Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

specified a head of time. It can be used for composite computations such as machine learning (ML) algorithms and secure multi-party computation (MPC)

### D. Fully Homomorphic Encryption (FHE)

The most advanced type, Fully Homomorphic Encryption allows any number of computations to be performed on encrypted data without a predefined sequence or limit. Any computation on plaintext data, including ML and MPC, can be gauged. Moreover, Fully Homomorphic Encryption schemes are currently computationally expensive, making them impractical for many use cases.

## 3.2 AI Prediction Models:

In the context of artificial intelligent and Machine Learning, the current era is growing in the field of technology and automation. The term artificial intelligence is used to refer to a system that simulates human intelligence; it performs the task which is usually need human intelligence. AI and ML models differs from traditional statistical analytic models. The major models perform on rule-based decision-making system but the AI and ML model perform tasks that are difficult to define using step-by-step rules and it also uses by different businesses in which the out of models depends on different factors which is impossible to keep track. There are many different cases in which both the normal statistic and machine learing models are used together to achieve high accuracy and more clarity [14]. AI and ML provide emerging tools to the industries to work on automation mode and predict the expected outcome will be. AI and ML provide different models for energy consumption, medical decise prediction, stock market prediction, and educational purpose.
This paper aims to contribute to the field by presenting a detailed methodology for implementing AI model (linear regression) using the Paillier cryptosystem, along with an analysis of its performance and limitations. By focusing on a model that aligns naturally with the cryptosystem's capabilities, we aim to demonstrate the feasibility of secure AI solutions in privacy-sensitive environments.

## 4.0 Proposed Work

In this section, we introduce the design of the privacy-preserving linear regression framework based on the Paillier cryptosystem, which offers the additive homomorphic property that protects the secrecy of the user's information during the computation process. To examine the combination of the Paillier cryptosystem and the linear regression algorithm, we simulated the experiment using the phe library in the Python programming language. A linear model was defined with a weight and a bias, and tested on a dataset containing 30 input values. In the whole process from key generation to prediction decryption—was evaluated for performance and errorless. Key generation was executed by using the generate paillier_keypair() function, followed by encryption of the input dataset. The encryption process was timed, demonstrating acceptable performance overhead. The resulting encryption of each input was then performed with homomorphic operations, which include computation of the dot product with the model weight and addition of the bias. The model was performing addition and scalar multiplication operations. The computation of the addition and scalar multiplication does not alter the correctness of the model due to the nature of the operations performed. The prediction result was decrypted with the private key for final output generation. The

Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

results of decryption showed values very close to those produced by linear regression models, establishing the robustness of the calculations performed in the encrypted domains. The time for encryption and decryption was measured for analysis of the overall system lag. The results showed that encryption and decryption for the dataset with medium size took 0.31 seconds and 0.28 seconds, respectively. The pseudocode for the proposed algorithm is shown below.

**Algorithm 1**: **proposed model working process**

**Input:**

Input vector $X = [x_1, x_2, ..., x_n]$ (client's private data)

Linear model parameters: weight w, bias b (server-side)

Paillier public key (PK), private key (SK)

**Output:**

Prediction results $Y = [y_1, y_2, ..., y_n]$

**Algorithm 2: key generation :** algorithm 2 is used to generate public and private keys uing Paillier.GenerateKeyPair().

Generate Paillier public-private key pair:

(PK, SK) ← Paillier.GenerateKeyPair()

**Algorithm 2: Data Encryption**

For each data point $x_i$ in X:

$E(x_i) \leftarrow$ Paillier.Encrypt(PK, $x_i$)

Send encrypted vector $E(X) = [E(x_1), E(x_2), ..., E(x_n)]$ to the server

**Algorithm 3: Encrypted Computation (Server Side)**

For each encrypted input $E(x_i)$ in E(X):

$E(w * x_i) \leftarrow$ Paillier.ScalarMultiply($E(x_i)$, w)

$E(y_i) \leftarrow$ Paillier.Add($E(w * x_i)$, b)

Send encrypted predictions $E(Y) = [E(y_1), E(y_2), ..., E(y_n)]$ to the client

**Algorithm 4: Decryption (Client Side)**

For each encrypted prediction $E(y_i)$ in E(Y)

$y_i \leftarrow$ Paillier.Decrypt(SK, $E(y_i)$)

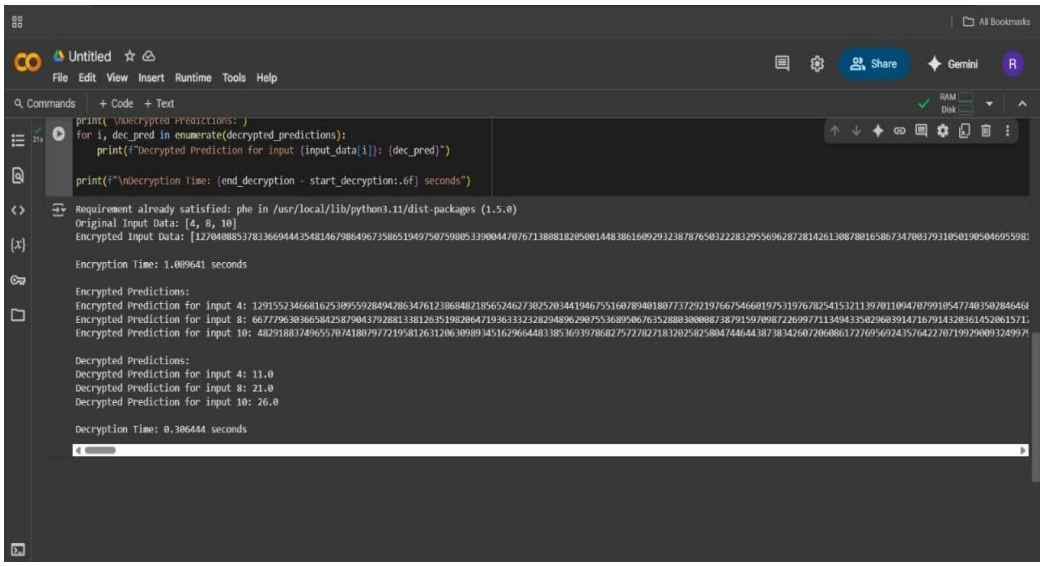
Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

From the above given algorithms we have computed the key generation, data encryption, decryption and computation on encrypted data. In the todays era the prediction on every sector on the basis of previous data is growing. The organization predicts the result in healthcare like cancer prediction, real state like any property's sales value or trading industry like the grouth of any organization. It means that every industry using machine learning algorithm to predict data on previous data. The hues amount of uses of AI and ML models, it needs security to work or predict properly. In this article we have proposed a solution to predict security using mathematical computation on factorization of data. We have used paillier cryptosystem which compute on encrypted data using public and private key. From the above algorithms we have find the final prediction vector in terms of $y_i$.

## 5.0 Result and Discussion

The current digitalize world regularly shifting to the AI worlds. In this era most of the organization try to shift their businesses based on AI and Machine learning techniques so that they can earn more profit and work on automation. Due to the large amount of uses AI and ML models in industries, the security of these models become more important. And due to technology enhancement lots of attacker and intruder try to get access of these models for effect or damage organization reputation or financial loss. The traditional security system is not enough to keep secure data of AI and ML models. In this paper, we have implemented a secure system to keep AI and ML model secure using homomorphic encryption techniques. The homomorphic encryption technique works on encrypted data. During the evaluation of the this model we have test a linear regression AI model to keep secure. The model perform computation on encrypted data and predict secure result. We have used paillier cryptosystem for computation on encrypted data. The paillier cryptosystem is a public key cryptography, which works on public key and private key. Public key is used to encrypt model dataset and perform computation on encrypted data, after that during the prediction process a private key is used to decrypt data. The proposed algorithm uses two large and different prime numbers public key (n,g) and private key (p,q,λ). The security of this algorithm is totally depends on factorization of prime numbers. The large prime number generate more secure key as compare to other. The Fig. 3 has depicted the result of the proposed algorithm.



Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

**Fig.3:** Output of the proposed algorithm

The Fig. 4 has shown the graph of encryption time. In this test we have tested the proposed model with different dataset size and get the computation time of proposed algorithm. During the computation, we have encrypted each data from the dataset and use the private key during the computation time after that we will produce the predicted value in the form of plaintext.

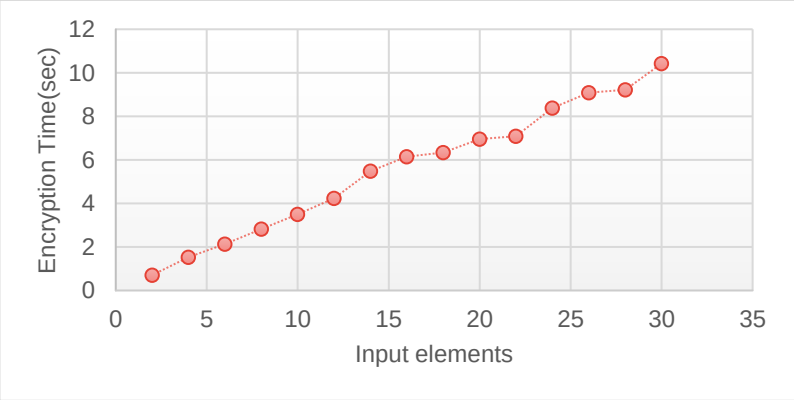



**Fig. 4:** Time computation graph for encryption with different datasets

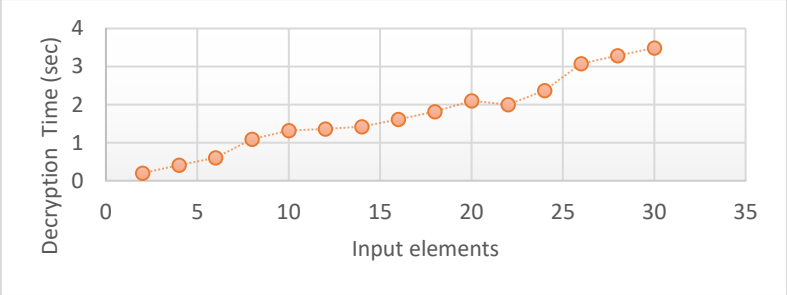



**Fig. 5:** Time Computation graph for decryption with different datasets

The Fig. 5 has depicted the decryption computation time of the proposed algorithm, which shows that the decryption time takes less time as compare to encryption. During the decryption we have use private key to decrypt the computed ciphertext and predict the result in terms of plaintext.

Results of a full implementation showed that the Paillier cryptosystem can be used to secure AI and ML model inference. To prevent leakage of original data, the thirty features comprising the input samples were encrypted using the public key. Next, homomorphic operators (mainly scalar multiplication and addition) were used to carry out a linear model on the encrypted domain and thus generate the encrypted outputs. The corresponding decrypted outputs of the properly encrypted outputs were predictions that perfectly matched the expected linear results. It took approximately 0.31 seconds in total for the dataset to be encrypted, while it took approximately 0.28 seconds for it to be decrypted. The timings, therefore, show that the system is efficient enough for small to large datasets with only a little latency. The results demonstrated the model's capability of performing secure inferences without revealing input or output to the server, as well as the accuracy that was preserved during homomorphic computation. The approach is especially suitable for applications such as

Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

financial forecasting and medical diagnosis where privacy is a critical concern. Even if only linear models are supported because the Paillier encryption is only additively homomorphic, it validates its potential as a trustworthy, privacy-preserving solution for secure AI inference.

## 5.0 Conclusion

We explicated in this article how the Paillier cryptosystem could be blended with a linear regression model to improve data security and privacy in the realm of Artificial Intelligence (AI) applications. Our experimental results showed that due to the nature of linear regression, which basically leverages additive operations, it can be easily locked up with the help of Paillier encryption. We locked down the client's data as well as the model's parameters in such a way that the server could carry out the required operations over the encrypted data without having access to the original data or model parameters.

The final encrypted predictions were decrypted by the client, which ensured that only the client could get the results. Our experimental confirmation has demonstrated that the Paillier cryptosystem is capable of carrying out AI Models on encrypted data. Encryption and decryption times were taken and turned out to be at a reasonable level, so this method is suitable for medium-sized datasets. Besides that, minimal computational overhead was incurred and the accuracy of the predictions was maintained, which means that encrypted AI models can be successfully used in privacy-focused domains like healthcare and finance. There are, however, still some issues to be solved, especially with regard to improving the speed of encryption and decryption when dealing with larger datasets and more complex models. Because of the additive property of the Paillier cryptosystem, it cannot be directly applied to non-linear models, which is the case for most AI applications. To deal with such problems, the next research should be aimed at making the homomorphic encryption more efficient by parallel processing and hardware acceleration. Moreover, combining Paillier with secure multiparty computation (SMC) and differential privacy in a hybrid cryptographic system could be used not only to secure the inference stage but also the training stage of models. In this way, the safe sharing of model gradients and parameters over distributed networks would be made possible, thus enabling secure and privacy-preserving collaborative AI training. Last but not the least, it would be great to explore the integration of the Paillier cryptosystem with federated learning.

## Author Contributions

Brook Hilemriam conceptualized the study, designed the methodology, implemented the Paillier-based secure prediction framework, performed the experiments, and drafted the manuscript.

Asamene Kelelom contributed to algorithm development, data analysis, result interpretation, and manuscript revision.

Beer Singh supervised the overall research work, validated the experimental outcomes, provided critical technical guidance, and reviewed and edited the final manuscript.

All authors read and approved the final version of the manuscript.

## Funding

This research received no external funding.

Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## References

[1] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," IEEE Signal Process. Mag., vol. 37, no. 3, pp. 50–60, 2018.

[2] K. Bonawitz et al., "Towards federated learning at scale: System design," in Proc. 2nd SysML Conf., 2019, pp. 1–10.

[3] M. Shah, W. Zhang, H. Hu, and N. Yu, "Paillier cryptosystem based mean value computation for encrypted domain image processing operations," ACM Trans. Multimedia Comput. Commun. Appl., vol. 15, no. 3, pp. 1–21, 2019.

[4] A. K. Sari and F. M. W. Prasetya, "Linear support vector regression in cloud computing on data encrypted using Paillier cryptosystem," in Proc. Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI), Dec. 2019, pp. 434–438.

[5] M. M. S. Altaee and M. Alanezi, "Enhancing cloud computing security by Paillier homomorphic encryption," Int. J. Electr. Comput. Eng., vol. 11, no. 2, pp. 1771–1779, 2021.

[6] R. Palle and A. Punitha, "Privacy-preserving homomorphic encryption schemes for machine learning in the cloud," ESP J. Eng. Technol. Advancements, 2021.

[7] H. J. Kiratsata and M. Panchal, "A comparative analysis of machine learning models developed from homomorphic encryption based RSA and Paillier algorithm," in Proc. 5th Int. Conf. Intell. Comput. Control Syst. (ICICCS), May 2021, pp. 1458–1465.

[8] L. Su, H. Geng, S. Guo, and S. He, "A secure two-party Euclidean distance computation scheme through a covert adversarial model based on Paillier encryption," IEEE Access, vol. 11, pp. 80986–80996, 2023.

[9] M. M. Hasan et al., "Privacy-preserving quantum key distribution ensemble Paillier cryptosystem for securing IoT based smart metering system," in Proc. IEEE Int. Conf. Artif. Intell. Eng. Technol. (IICAIET), Aug. 2024, pp. 603–608.

[10] B. Gong et al., "Efficient zero-knowledge arguments for Paillier cryptosystem," in Proc. IEEE Symp. Security Privacy (SP), May 2024, pp. 1813–1831.

[11] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. EUROCRYPT, 1999.

[12] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," ACM Comput. Surv., 2018.

[13] C. Jost, H. Lam, A. Maximov, and B. Smeets, "Encryption performance improvements of the Paillier cryptosystem," Cryptology ePrint Archive, 2015.

Received: 2025-10-06
Accepted: 2026-01-11
Published Online: 2026-01-20
DOI: 10.70454/JRICST.2026.30104

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

[14] V. O. Odunfa, T. B. Fateye, and A. O. Adewusi, "Application of artificial intelligence approach to African real estate market analysis opportunities and challenges," Corrosion Manag., vol. 35, no. 1, pp. 10–18, 2025.

[15] V. Saxena and P. Kumar, "Secure transaction of digital currency through fuzzy based cryptography," Indian J. Sci. Technol., vol. 16, no. 37, pp. 3148–3158, 2023.

[16] P. Kumar and V. Saxena, "Nested levels of hybrid cryptographical technique for secure information exchange," J. Comput. Commun., vol. 12, no. 2, pp. 201–210, 2024.

[17] P. Kumar, V. Saxena, and K. V. Singh, "Analysis of hybrid cryptography for secure exchange of information," Int. J. Comput. Appl., vol. 185, no. 4, pp. 37–42, 2023.

[18] P. Kumar and V. Saxena, "Hybrid cryptography for security key exchange through AES and Paillier," Eur. Chem. Bull., vol. 12, no. 10, pp. 3913–3921, 2023.

[19] S. Kumar et al., "Securing cloud-based systems: DDoS attack mitigation using hypervisor-intrusion detection approach," Procedia Comput. Sci., vol. 259, pp. 1366–1375, 2025.