International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Performance Enhancement in Cloud Based Network Using Polynomial Encryption and Deep Learning

Prof. Ajit Singh[1], Geeta Rani* [2], Saya[3]

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 22/03/2024

Abstract: Present paper provides the conceptual framework for enhancement of performance in cloud -based network using the concepts of polynomial encryption and deep learning. The earlier techniques like RSA, AES and DES etc. used for security systems were slow and provided limited security. In order to enhance the performance and safety of cloud servers, polynomial encryption mechanism with the concept of deep learning has been developed by modifying the existing data encryption techniques to allow novel hybrid cryptography processes. This proposed versatile security mechanism is capable to deal with denial of service, brute force attack and man in middle attack and also capable to classify different type of attacks for the protection of cloud-based networks. The deep learning approach used to restrict invalid data transmission along with data encryption. Further, the mathematical calculations shows that the proposed mechanism provides 85% accuracy whereas the conventional mechanism having accuracy of 75%. Similarly, the value of other parameters like security, precision, recall value and F1-Score of proposed mechanism are better than existing conventional mechanism. Hence, system based on the proposed mechanism is having more efficient, flexible and scalable than the existing one.

Keywords: *Cloud Computing, Polynomial Encryption, Security, Confusion Matrix, Accuracy parameters, Deep Learning.*

1. Introduction

Computing on the cloud is making widespread inroads into the technological sector in this modern age of information and technology. Academic authorities, business giants, officials of the government, and IT corporations have all raised serious concerns over the safety of cloud computing and the challenges it faces in terms of entrance barriers [1]. Some of these include the protection of personal data, the accessibility of services, the selection of service providers, and the dissemination of reputational outcomes. These issues are the outcome of preexisting issues as well as newly formulated needs for cloud computing capabilities such as scalability, resource sharing, and virtualization [2]. Both the kind of deployment and the model of service delivery are significant aspects to consider while classifying them. The process of moving information to & from cloud, there is still a possibility that digital assets may be compromised. However, it was emphasized that there was a need for increased online safety measures. At the moment, the primary emphasis of research is on finding ways to improve both the safety and the efficiency of cloud-based remote learning systems [3]. There has been a great deal of studies conducted on the topic of using cloud computing for online instruction. Researchers have already determined that there are issues with both the performance and the security of the data [4]. It is essential for the movement of digital data from one location to another to take place quickly and securely. During the time that data is in transit, digital content assets need to be encrypted and compressed. The researchers used a content replacement approach to cut down the size of the packet [5].

[1,2,3]*Department of Computer Science and Engineering, BPS Mahila Vishwavidyalaya Khanpur Kalan, Sonepat-131305, Haryana, India*

1.1. Basic Techniques used for Encryption

Algorithms utilize a secret key to change data such that it can be decrypted using the decryption key even though the encrypted data will look random. Symmetric and asymmetric encryption is the two main forms of encryption currently in use. The term "key-based encryption" describes a system where the same key is utilized for both the enciphering and deciphering processes. The commonly used encryption techniques are DES, AES, and RSA.

1.1.1. Cloud Computing

The use of internet infrastructure to deliver computer services that were previously unreachable provides the way to enhance efficiency, scalability and rate of innovation [6]. Hosting websites on internet, backing up and managing data, developing databases and applications, as well as providing corporate insight and analytics are the examples of such services [7]. In cloud computing, data is kept on remote servers and can be accessed from any device as long as it has an Internet connection. The fact that anybody is able to make use of Google Cloud makes it an excellent illustration of a public cloud service [8]. At every stage of the application development process, Google's hardware is used. Operations for large clouds are often distributed over a large number of distinct data centre's. NIST recognizes three fundamental cloud computing service models: IaaS, PaaS, SaaS, and PaaS [9].

It is feasible to execute programs by using IaaS rather than

enclosing them in SaaS [10]. Additionally, it is convenient to run applications and have direct access to them without going via SaaS in the first place. Computing in the cloud may be arranged into number distinct categories, most of common are public clouds, private clouds, hybrid clouds, and many clouds. IaaS, PaaS, and SaaS are the three primary categories of cloud computing services.

1.1.2. Polynomial Encryption

Polynomials are used to represent numerical results of calculations through a wide range of academic disciplines as well as being used as "building blocks" in polynomial expressions and rational expressions. The polynomial encryption public key cryptosystem [11] commonly known as the polynomial encryption method which is based on the shortest vector problem in a lattice, as opposed to RSA and ECC [2]. The foundation of this strategy is the ability to factor particular polynomials in a truncated polynomial ring into a quotient of two polynomials with exceedingly small coefficients [12]. The algorithmic challenge of lattice reduction is closely connected to breaking the cryptosystem, but it is not the same. Some disclosed attacks may be prevented with careful parameter selection. In compared to other asymmetric encryption methods such as RSA, ElGamal, and elliptic curve cryptography, speed of both encryption and decryption is greatly improved by use of just elementary polynomial multiplication. Polynomial encryption, on the other hand, has not been subjected to the same level of cryptographic scrutiny as other methods [13].

Polynomial interpolation, used to factories cryptographic issues and counter numerous assaults, formed the basis of a detailed method described for the field. Lagrange Interpolation was the standard method of key management for most pioneers. Interpolation is often used in cryptography because of its irreversible and puzzling feature [14]. The ECC algorithm was modified as a result the Interpolation method's integration into it and requires a compromise between speed and memory. The multi-factor authentication system uses the Newton interpolation algorithm. Bisection was employed to produce a random sequence for picture encryption. However, it was found to be vulnerable due to an attack on the XOR process [15].

The two main types of cryptosystems are used for security today: newer ones and older ones. The two processes—confusion and diffusion—run in tandem in contemporary systems but independently in older ones. The algorithms are vulnerable to being cracked by chaotic, unsupervised processing. Traditional research methods depend heavily on ambiguity and therefore. Chebyshev polynomials were also used in the development of public-key cryptosystems by academics [19]. To improve security, the authors devised a Chebyshev-maps-based encryption technique in which the AES algorithm was combined with chaotic maps. The disadvantages of maps have been detailed. The Chebyshev polynomial, which based on chaos theory, was used to encrypt the images [16]. The goal of broadcast encryption is to ensure that only members of the intended audience are able to decipher the encoded material by having it disseminated over public channels. However, they had to cope with the trade-off between security and computational complexity by embedding a broadcast strategy within polynomial interpolation algorithms to make them safer and more adaptable [17].

1.2. Deep Learning

Along with representation learning and artificial neural networks (ANN), Deep Learning (DL) is a member of a larger family of ML methods. The three main methods of learning are supervised, semi-supervised, and unsupervised. The following are some examples of DL architectures in action: CV, SR, NLP, MT, belief networks, reinforcement learning, RNN, CNN, and transformers [18]. ANN owes a debt to IP and decentralized communication nodes seen in biological systems. There are many key ways in which ANNs differ from biological brains. The brains of most living things are dynamic and analogue. In contrast to ANN, which tends to be static and symbolic. A multi-layer network training method is what the term "deep learning" alludes to [19]. Deep learning is a variant that guarantees theoretical universality under modest circumstances, is concerned with present-day applications and efficient implementations, and uses limitless layers of bounded size. Since precise adherence to physiologically informed connectionist models are less essential than efficiency, trainability, and interpretability in DL, the layers themselves may be extremely different. Deep learning, in contrast to conventional machine learning methods, requires less data preparation. These algorithms automate feature extraction by consuming and processing unstructured data such as text and photographs. Therefore, reducing the need for human professionals [20]. Deep neural network-based machine learning techniques shown exceptional success and widely utilized to analyses huge data in many fields. However, the raw data is typically privacy sensitive and cannot be used for training the models.

Table 1. Comparison of Security Techniques

Techniques	***Principle***	***Security***	***Loopholes***
RSA	RSA algorithm is example of asymmetric cryptographic method that calls for a pair of keys—public and private one [2, 12, 14].	A pair of keys, a public and a private one, is needed for RSA to work. The public key is shared with the world to encrypt messages.	RSA uses just asymmetric encryption but symmetric and asymmetric encryptions are both required for complete encryption, RSA may fail.
DES	As block cipher algorithm, Data DES encrypts plaintext in 64-bit blocks with 48-bit keys [4].	When weaker form of encryption is required, DES is the algorithm of choice.	DES algorithm's 56-bit key size is probably its biggest drawback.
AES	AES is a 128-bit block/chunk symmetric block cypher. Each block is encrypted using a key of either 128, 192, or 256 bits in length. [5].	This highly effective security algorithm is compatible with both hardware and software implementations.	The primary shortcoming of AES symmetric key encryption is the need to symmetric encryption keys using an asymmetric algorithm such as RSA.
Polynomial encryption	Polynomial encryption provides unique security. This mechanism is efficient and scalable [11, 15].	It is providing high performance.	The limitation of research work is that it provides limited security.
Deep Learning	Learning by example is second nature to humans, and DL is an ML technique that teaches computers to do the same. [3]	Enables the use of an AI method for detection and categorization As we've seen, Deep Learning algorithms' primary strength is their endeavor to gradually learn high-level characteristics from data.	Obtaining accuracy and performance is challenging. To outperform alternative methods, a massive data set is required.

Thanks to recent developments in polynomial encryption, we can safely apply DL techniques to encrypted data and get back encrypted results. There are many benefits to utilizing polynomial encryption techniques, only simple arithmetic operations can be successfully performed over encrypted data, and complicated functions like sigmoid functions utilized in neural networks are impractical with existing polynomial encryption systems. [21].

The above table presented the comparative analysis of different types of security techniques. In table-1, the deep learning is expected to reduce attack probability. It is observed that the above table that the AES is providing better security as compared to DES and RSA whereas polynomial encryption saves time during data encryption. Moreover, the deep learning approach enhances and provides a smart security system. But training and testing are time-consuming and operations are also complex in deep learning. The polynomial encryption should be used with Deep Learning to provide a smart and efficient security system for the cloud environment as the AES and DL techniques are more complex.

1.3. Deep Learning Techniques

The most commonly used techniques of the Deep Learning are given as under:

- Conventional Neural Network (CNN).

- Recurrent Neural Network (RNN)
- Artificial Neural Network (ANN)
- Generative Adversarial Networks.
- Self-Organizing Maps.
- Boltzmann Machines.
- Reinforcement Learning

And their brief comparisons are presented in the following table:

Table 2. Comparison of Deep Learning Techniques [22]

Parameter	***ANN***	***CNN***	***RNN***
Data Types	Textuals	Images	Sequences
Spatial recognitions	N	Y	N
Recurrent connection	N	N	Y
Drawbacks	Hardware dependency	Large training dataset	Slow and complex training
Use	Prediction	Image classification and recognition	NLP

1.4. Confusion Matrix and Parameters

The nature of the business issue being addressed should frequently guide the selection of a performance indicator. Suppose you have a dataset containing 100 instances and you have classified each one using your model. Figure 1 is called a confusion matrix may be used to plot the projected classification against the actual classification [23].

		Real Label	
		Positive	***Negative***
Predicted Label	***Positive***	True Positive (TP)	False Positive (FP)
	Negative	False Negative (FN)	True Negative (TN)

Fig. 1. Confusion matrix and Accuracy Parameters

1.4.1. Accuracy

Accuracy is a good heuristic for gauging the quality of a model's training and its potential future performance. However, it does not provide specifics on how to apply it to the issue at hand.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

When there is a large disparity across classes, performance metrics that rely heavily on accuracy tend to suffer. Apply the aforementioned confusion matrix to the dataset. Assume that the negatives represent legitimate purchases and the positives represent fraudulent ones. If you want to know how often you're right across all subject areas, accuracy will tell you.

1.4.2. Precision

When the cost of a false positive is large, accuracy is beneficial. Let's pretend, therefore, that finding skin cancer is the issue. There will be several further examinations and pressure. After being swamped with false alarms, people responsible for monitoring the data will eventually learn to disregard them when the false positive rate is high.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

1.4.3. Recall

A significant amount of damage may result from a false negative. The end will be ours if you err. Your best efforts to prevent something will be in vain if false negatives happen often. A false negative is when you go into the woods and ignore the rustle of leaves and end up being devoured by a bear. You wouldn't want to keep a model that accidentally allowed in nuclear weapons. You should get rid of your model if chipmunks are keeping you up at night. If you, like the majority of people, want to avoid being devoured by a bear while simultaneously sleeping well, it is desirable to optimize for an evaluation metric that having both accuracy and recall.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

1.4.4. F1 Score

Like the strange way that adding and multiplying only combine two ingredients to make a new dish, F1 is a total assessment of a model's accuracy that takes precision and recall into account. To restate, a high F1 score indicates that you are upright at identifying real threats and are unconcerned by false alarms. A perfect model would have an F1 score of 1, whereas a total failure would be indicated by a score of 0.

$$\text{F1} - \text{Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

2. Existing RNN Based Security System

When compared with the ANN model, the mechanisms of RNN were used in conventional research work that concentrated on the protection of data through the

classification of different types of attacks. The LSTM (Long short-term memory network) model is taken into consideration by this model for the classification process. It uses LSTM for attack classification with high accuracy.

When training and testing, a large dataset of attacks is taken into consideration. During the training process, hidden layers, fully connected layers and sequence layers are utilized to increase accuracy and drop layers are utilized to decrease the probability of accuracy. Following the RNN model's training phase, the testing phase involves the classification of attacks by considering the accuracy of attack detection and classification.

2.1. Algorithm

The RNN algorithm includes following steps for the protection of data through the classification of different types of attacks:

Step 1: Get data set for training

Step 2: Initialize LSTM training parameters

Step 3: Preprocess dataset before training

Step 4: Set 70% dataset for training

Step 5: Set 30% dataset for testing

Step 6: Initialize training parameters such as epochs, iteration, dropout layer, dense layer

Step 7: Train using LSTM based network

Step 8: Apply testing and get confusion matrix

Step 9: Get accuracy, recall, f1 score and precision

Step 10: Evaluate performance and accuracy.

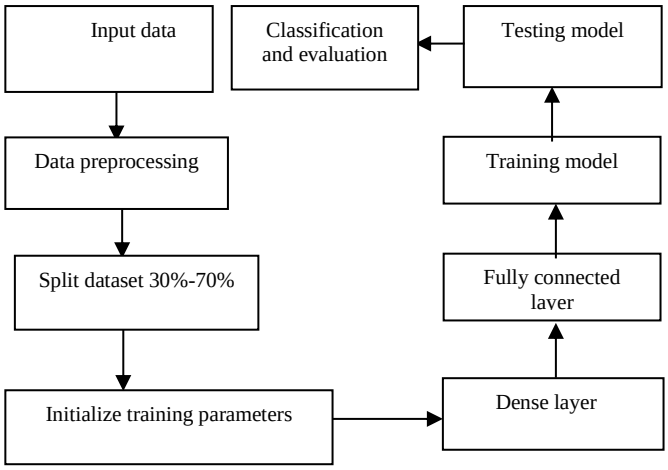

Fig. 2. RNN Based Classification

Input: A data set consisting of assaults and regular data transfer are taken into consideration for training.

Output: The results of training and testing a model are referred to as the model's accuracy, recall value, precision, and recall value.

Strength: When an attack is classified, the system's level of security is increased, and the level of accuracy provided by such a system is superior to that of the ANN model.

2.2. Limitations

This approach takes lot of time since training and testing take while when the dataset is big. The limitations of this approach are given as under:

Layer compatibility.

Complication of implementation.

Performance less so to do data filter.

2.3. Confusion matrix during attack classification on unfiltered dataset

The confusion matrix during attacks is classified based on unfiltered dataset in the different ways shown below in the table 2:

Table 3. Confusion Matrix during Attack Classification on Unfiltered Dataset

	Class 1	***Class 2***	***Class 3***	***Class 4***
Class 1	1430	369	360	321
Class 2	332	1236	306	1699
Class 3	4556	5450	360	4014
Class 4	856	1780	1451	1420

True positive (TP): 4446

Overall Accuracy: 75.14%

Table 4. Parameter of Unfiltered

Class	***n (Truth)***	***n (Classified)***	***Accuracy***	***Precision***	***Recall***	***F1 Score***
1	7174	2480	73.81 %	0.58	0.20	0.30
2	8835	3573	61.7%	0.35	0.14	0.20
3	2477	1438	37.79 %	0.025	0.15	0.43
4	7454	5507	60.98 %	0.26	0.19	0.22

In above table, the overall accuracy of unfiltered dataset is 75.42%. The overall precision of unfiltered dataset is 0.40. The overall Recall of unfiltered dataset is 0.17. The overall F1 Score of unfiltered datasets is 0.22. Hence, if security is improved then the performance gets decreased. On other hand, if performance factor is considered then security get

decreased.

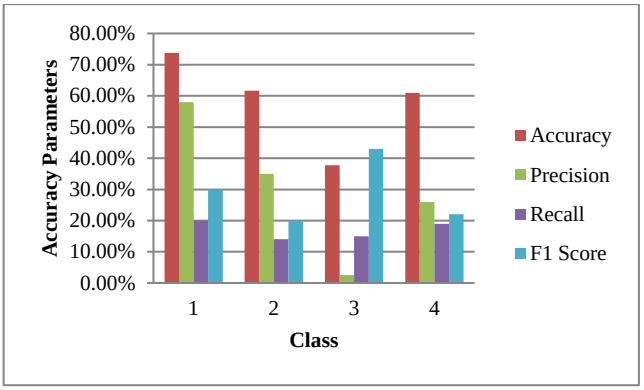

Fig. 3. Comparison of Parameters

3. Proposed Mechanism

The limited attacks were considered in the conventional system and the encryption of data in huge size of files was time consuming. Data encryption could only restrict unauthentic user to understand data but it could not restrict them from destroying it. The conventional system considered limited protocol where data was transferred on specific port number but there was more threat to well-known route. Each and every time lot of the time was wasted in verification of packet when transaction is initiated from same route. Predefined encryption mechanisms are easy to crack. The proposed mechanism overcomes the above said problems and based on concepts of polynomial encryption, compression and deep learning. It provides filtered compressed dataset by content replacement-based compression and considers user defined polynomial encryption to reduce chances of cracking. There is no need to verify packet at each transmission as LSTM based deep learning approach allow authentic transmission by considering previous experience and classifying attacks.

The following flowchart shows the process flow of proposed work

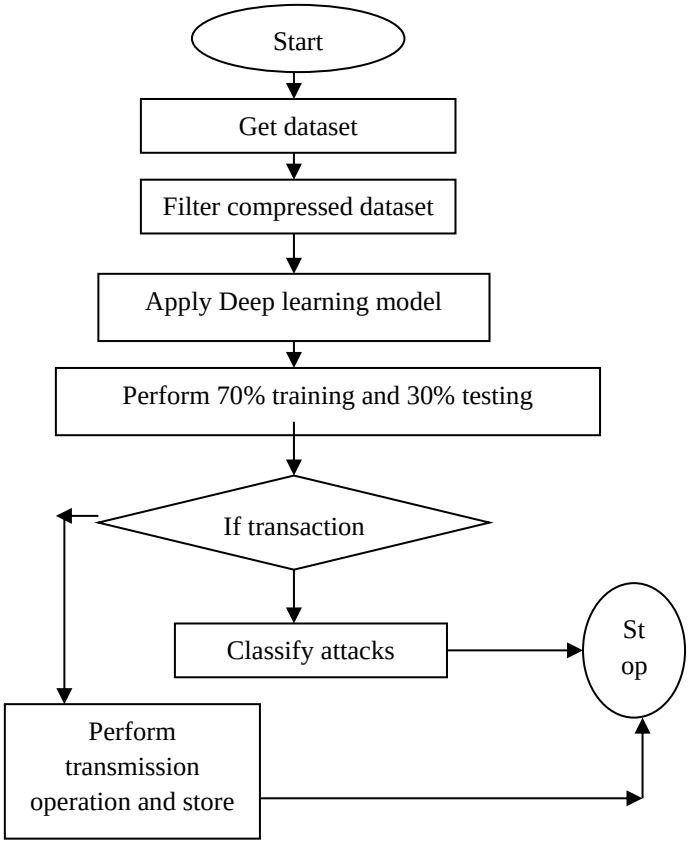

Fig. 4. Process Flow of Proposed Work

3.1. Polynomial Encryption:

The polynomial encryption involves the following steps:

Step 1: Get the Data for encryption Z

Step 2: Loop

Step 3: Get character C from Z

Step 4: Get ASCII (AC) code of c

Step 5: Apply polynomial equation to get encrypted data (ED)

Step 6: ED = AC+ 4

Step 7: End loop

3.2. Polynomial Decryption

The polynomial decryption process involves the following steps:

Step 1: Get the Data for decryption es

Step 2: Loop

Step 3: Get character ce from ES (encrypted string)

Step 4: Get ASCII (AC) code of ce

Step 5: Apply polynomial equation to get decrypted data (DD)

Step 6: DD = (AC – 4)/2

Step 7: End loop

Concatenate dd and get decrypted string (ds)

3.3. Mathematic example

Suppose data for encryption is 4,

And polynomial equation for encryption is

$$x^2 + 3$$

Then encrypted data is

$$F(x) = x^2 + 3$$

Example: (4*4) + 3 =19

In this way encrypted data is 19 when polynomial equation is x2+3

At the decryption time the decryption equation is

$$f(enc) = \sqrt{(enc - 3)}$$

Example: √(19-3)= √16= 4

The proposed system provided the security at multiple layers. Initially data has been processed by compression and polynomial encryption and there is machine learning mechanism that classifies attacks and normal data delivery. The Fig3 is presenting how data is filtered using machine learning approach where the compressed and encrypted data is passed to machine learning mechanism to take decisions for considering the rained neural network. If transaction is normal then operation proceeds otherwise if there is any attack then categories attack and transmission is restricted. In this way the proposed mechanism provided multilayered security.

4. Result and Discussion

The theoretical foundations of polynomial encryption are for securing cloud-based networks. The researchers believe that polynomial encryption may be used to make cloud servers safer if existing data encryption standards are modified to allow for unique hybrid cryptography approaches. Consequently, a large number of unrecognized security concerns have been emerged [20]. The significant changes have been made to the manner in which organizations approach with the introduction of cloud computing for offering IT infrastructure as a service.

4.1. Confusion Matrix During Attack Classification on Unfiltered Dataset

Considering incoming packets machine learning mechanism has been developed in order to categorize attacks. There are 3 categories of attack. Machine learning mechanism is classifying attack categories and normal data packets.

Table 5. Confusion Matrix during Attack Classification on Unfiltered Dataset

	Class 1	***Class 2***	***Class 3***	***Normal***
Class 1	1432	124	156	157
Class 2	175	1524	176	165
Class 3	143	198	1456	176
Normal	250	154	212	1502

True Positive: 5914 and

Overall Accuracy: 73.93%

Table 6. Accuracy for Unfiltered

Class	***n (Truth)***	***n (Classified)***	***Accuracy***	***Precision***	***Recall***	***F1 Score***
1	2000	1869	87.44 %	0.77	0.72	0.74
2	2000	2040	87.6%	0.75	0.76	0.75
3	2000	1973	87.74 %	0.74	0.73	0.73
4	2000	2118	86.08 %	0.71	0.75	0.73

4.2. Confusion Matrix During Attack Classification on Filtered Dataset

The machine learning mechanism has been developed to categorize the attacks by considering incoming packets. There are three categories of attacks and the mechanism is able to classify the attack categories and normal data packets.

Table 7. Confusion Matrix during Attack Classification on Filtered Dataset

	Class 1	***Class 2***	***Class 3***	***Normal***
Class 1	1734	76	93	91
Class 2	72	1749	88	82
Class 3	98	93	1717	73
Normal	96	82	102	1754

True Positive: 6954

Overall Accuracy: 86.93%

Table 8. Accuracy for Filtered

Class	*n (Truth)*	*n (Classified)*	*Accuracy*	*Precision*	*Recall*	*F1 Score*
1	2000	1994	93.43 %	0.87	0.87	0.87
2	2000	1991	93.84 %	0.88	0.87	0.88
3	2000	1981	93.16 %	0.87	0.86	0.86
4	2000	2034	93.43 %	0.86	0.88	0.87

5. Comparison Analysis of Parameters

Table shows the outcomes of each class's inventory of the quality of finished work and the priority of future assignments (1, 2, 3, and 4). The filtered data has been proven to be more accurate than the original unfiltered data.

5.1. Accuracy

The compare of accuracy value for the unfiltered dataset and filtered dataset given as below:

Table 9. Comparison of Accuracy

Class	*Unfiltered*	*Filtered*
1	87.44%	93.43%
2	87.6%	93.84%
3	87.74%	93.16%
4	86.08%	93.43%

Using the information in table 8, we can now compare the filtered and unfiltered datasets to demonstrate improved accuracy of the filtered version in figure 5.

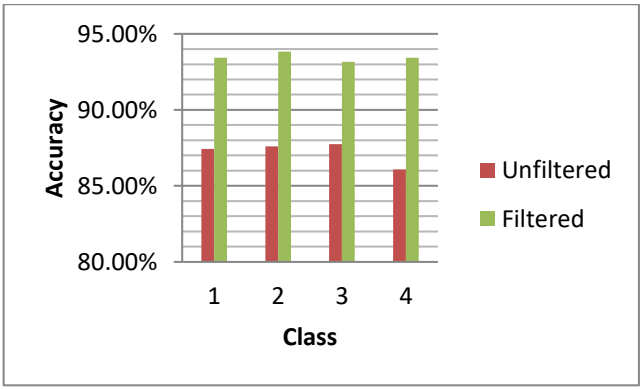

Fig. 5. Comparison of Accuracy

Table 10 shows the reliability of previous and anticipated performance for grades 1, 2, 3, and 4. The filtered dataset has substantially greater accuracy than the original one.

5.2. Precision

The compare of precision value for the unfiltered dataset and filtered dataset given as below:

Table 10. Comparison of Precision

Class	*Unfiltered*	*Filtered*
1	0.77	0.87
2	0.75	0.88
3	0.74	0.87
4	0.71	0.86

When comparing the filtered and unfiltered data sets, recall in the filtered dataset is seen in figure 6.

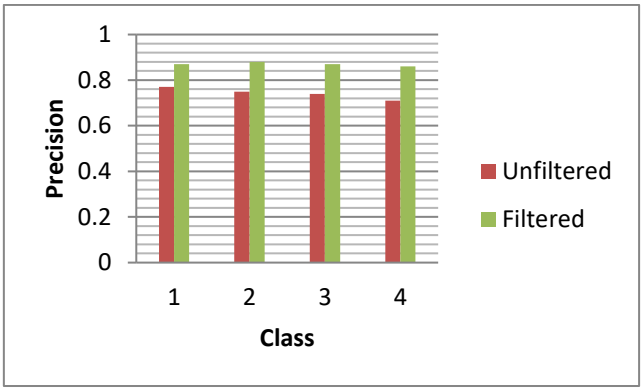

Fig. 6. Comparison of Precision

Table 11 displays comparing recall values of the existing work with the proposed work for classes 1, 2, 3, & 4. One difference between the filtered and unfiltered is shown in Recall value.

5.3. Recall Value

The compare of recall for the unfiltered and filtered given as below:

Table 11. Comparison of Recall

Class	*Unfiltered*	*Filtered*
1	0.72	0.87
2	0.76	0.87
3	0.73	0.86
4	0.75	0.88

In table 10 shows, how filtered performs in terms of recall by comparing with unfiltered dataset in figure 7. We can get an idea of how well it performs in terms of recall by comparing filtered (figure 7) to unfiltered (table 11),

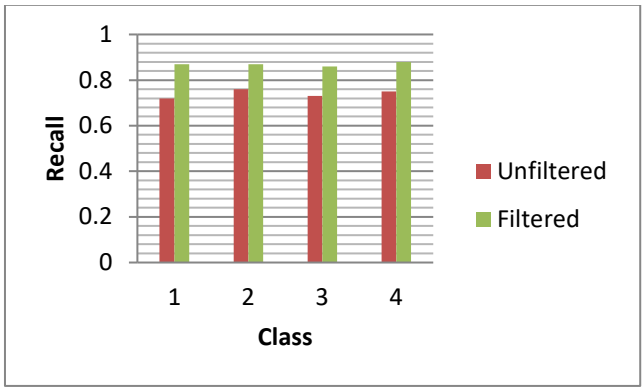

Fig. 7. Comparison of Recall Value

Completed and upcoming projects' F1-scores across all four categories are shown in Table 12. When compared to an unfiltered dataset, filtered one has a higher F1-Score.

5.4. F1- Score

The compare of F1-score value for the unfiltered and filtered dataset given as below:

Table 12. Comparison of F1-score

Class	*Unfiltered*	*Filtered*
1	0.74	0.87
2	0.75	0.88
3	0.73	0.86
4	0.73	0.87

Figure 8 was created based on data in table 12 to demonstrate the difference between the filtered and unfiltered F1-scores.

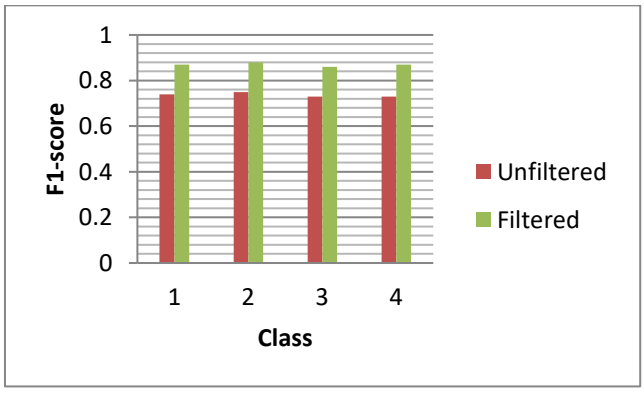

Fig. 8. Comparison of F1-Score

As seen in the above, it is anticipated that deep learning would lower assault probability. The proposed solution already provides security on numerous different levels. Compression and polynomial encryption were used to handle data in the beginning, and the machine learning system is identifying assaults and routine data transmission. The process of filtering data using a machine learning technique, which shows how data is compressed and encrypted before being submitted to a machine learning model, where judgments are made taking into consideration a trained neural network. If the transaction is regular, then the process will continue, but if there is any kind of attack, then the type of attack will be provided, and transmission will be prohibited. The suggested methodology has accomplished this by providing security at many layers.

6. Performance Comparison

The following table shows the performance comparison between existing technique and proposed technique:

Table 12. Comparison Analysis of Parameters

Sr.No.	*Parameters*	*Existing Technique*	*Proposed Technique*
1	Security	Limited single layered security	High Multilayer security
2	Accuracy	73.93%	86.93%
3	Precision	0.7425	0.87
4	Recall	0.74	0.87
5	F1-Score	0.7375	0.87

The above table shows that the value of parameters like security, Accuracy precision, recall and F1-Score of proposed mechanism are better than existing mechanism. Hence, the proposed mechanism based system is more accurate, secure and scalable than existing one.

7. Conclusion

The conventional data security mechanisms such as DES, AES, and RSA are capable of providing security using the complex algorithm and the time consumption for execution of such algorithms is high. It is anticipated that deep learning would lower assault probability. On the other hand, during Deep Learning the training of the data set required existing records to train the machine to provide security whereas the polynomial encryption is fast but it is providing limited security. Thus, there remains a need to integrate polynomial encryption and deep learning where both could work together to enhance performance and security. In order to enhance performance and safety of cloud servers, polynomial encryption mechanism with the concept of deep learning has been developed by modifying the existing data encryption standards to allow novel hybrid cryptography processes. This proposed versatile security mechanism is capable to deal with denial of service, brute force attack and man in middle attack and also capable to classify different type of attacks for the

protection of cloud-based networks. The integration of polynomial encryption and deep learning are used for classification of the different types of attacks to secure the data from unauthorized user and transaction is normal then operation proceeds but if there is any attack then category of attack is presented and transmission is restricted. In this way the proposed mechanism provided multilayered security. Moreover, it has been observed that the proposed mechanism providing better value of accuracy, precision, recall value and f1-score as compared to the conventional mechanism which makes the proposed mechanism-based system is more efficient and secure than existing one.

The integration of polynomial encryption with deep learning holds tremendous promise for enhancing cloud security across various fronts. From optimizing encryption schemes to advancing anomaly detection and enabling privacy-preserving machine learning, the synergistic combination of polynomial encryption and deep learning presents a paradigm shift in cloud security practices. As organizations continue to embrace cloud computing for their critical workloads, leveraging these innovative technologies will be essential for mitigating security risks and ensuring confidentiality, integrity, and availability of data in cloud.

8. Future Scope

The future scope of employing polynomial encryption in conjunction with deep learning for enhancing cloud security is poised to revolutionize data protection in cloud environments. The polynomial encryption, a cutting-edge cryptographic technique, offers robust protection against unauthorized access and data breaches by encrypting sensitive information with complex mathematical polynomials. When integrated with deep learning algorithms, this encryption method presents an innovative approach to bolstering cloud security. One significant avenue for exploration lies in leveraging deep learning algorithms to optimize polynomial encryption schemes for cloud environments. Deep learning techniques, with their ability to analyze complex patterns and relationships within data can be utilized to enhance the efficiency and scalability of polynomial encryption techniques. By training deep learning models on large-scale datasets of encrypted data, researchers can develop novel encryption schemes tailored to the specific requirements and constraints of cloud computing environments. These optimized encryption schemes can offer superior performance in terms of computational efficiency, scalability, and resistance to cryptographic attacks, thereby enhancing the overall security posture of cloud systems. Furthermore, the integration of deep learning with polynomial encryption holds promise for advancing anomaly detection and intrusion detection systems in cloud environments. Deep learning algorithms, particularly CNNs and RNNs, excel at detecting subtle patterns and anomalies within complex datasets. By applying deep learning techniques to encrypted data streams within the cloud, organizations can enhance their ability to identify and mitigate security threats in real-time. This proactive approach to security monitoring can significantly reduce the risk of data breaches and unauthorized access, thereby bolstering the trust and confidence of cloud users. Moreover, the combination of polynomial encryption and deep learning opens up new possibilities for privacy-preserving machine learning in the cloud. Traditional machine learning algorithms typically require access to plaintext data for model training, raising privacy concerns regarding the confidentiality of sensitive information. By employing polynomial encryption to encrypt data while preserving its utility for machine learning tasks, organizations can ensure data privacy and confidentiality in cloud-based machine learning workflows. This paradigm shift towards privacy-preserving machine learning holds immense potential for enabling collaborative data analysis and knowledge sharing across disparate organizations while safeguarding individual privacy rights.

References

[1] Z. Brakerski, “Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP,” Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 868–886, 2012. doi: 10.1007/978-3-642-32009-5_50.

[2] T. Plantard, W. Susilo, and Z. Zhang, “Fully Homomorphic Encryption Using Hidden Ideal Lattice,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 12. Institute of Electrical and Electronics Engineers (IEEE), pp. 2127–2137, Dec. 2013. doi: 10.1109/tifs.2013.2287732.

[3] G. Ye, C. Pan, X. Huang, and Q. Mei, “An efficient pixel-level chaotic image encryption algorithm,” Nonlinear Dynamics, vol. 94, no. 1. Springer Science and Business Media LLC, pp. 745–756, Jun. 05, 2018. doi: 10.1007/s11071-018-4391-y.

[4] H. Diab, “An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations,” IEEE Access, vol. 6. Institute of Electrical and Electronics Engineers (IEEE), pp. 42227–42244, 2018. doi: 10.1109/access.2018.2858839.

[5] A. Fu, S. Li, S. Yu, Y. Zhang, and Y. Sun, “Privacy-preserving composite modular exponentiation outsourcing with optimal checkability in single untrusted cloud server,” Journal of Network and Computer Applications, vol. 118. Elsevier BV, pp. 102–112, Sep. 2018. doi: 10.1016/j.jnca.2018.06.003.

[6] M. Wazid, S. Zeadally, and A. K. Das, "Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions," IEEE Consumer Electronics Magazine, vol. 8, no. 2. Institute of Electrical and Electronics Engineers (IEEE), pp. 56–60, Mar. 2019. doi: 10.1109/mce.2018.2881291.

[7] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," Optics and Lasers in Engineering, vol. 115. Elsevier BV, pp. 7–20, Apr. 2019. doi: 10.1016/j.optlaseng.2018.11.015.

[8] N. Hasan and A. Farhan, "Security Improve in ZigBee Protocol Based on RSA Public Algorithm in WSN," Engineering and Technology Journal, vol. 37, no. 3B. University of Technology, pp. 67–73, Oct. 25, 2019. doi: 10.30684/etj.37.3b.1.

[9] W. Liu, S. Fan, A. Khalid, C. Rafferty, and M. O'Neill, "Optimized Schoolbook Polynomial Multiplication for Compact Lattice-Based Cryptography on FPGA," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 10. Institute of Electrical and Electronics Engineers (IEEE), pp. 2459–2463, Oct. 2019. doi: 10.1109/tvlsi.2019.2922999.

[10] D. Harvey and J. van der Hoeven, "Faster polynomial multiplication over finite fields using cyclotomic coefficient rings," Journal of Complexity, vol. 54. Elsevier BV, p. 101404, Oct. 2019. doi: 10.1016/j.jco.2019.03.004.

[11] L. Liu, Y. Lei, and D. Wang, "A Fast Chaotic Image Encryption Scheme With Simultaneous Permutation-Diffusion Operation," IEEE Access, vol. 8. Institute of Electrical and Electronics Engineers (IEEE), pp. 27361–27374, 2020. doi: 10.1109/access.2020.2971759.

[12] Koppanati, Ramakrishna & Kumar, Krishan. P-MEC: "Polynomial Congruence-Based Multimedia Encryption Technique Over Cloud". IEEE Consumer Electronics Magazine. PP. 1-1. 10.1109/MCE.2020.3003127.(2020).

[13] R. K. Salih and M. Sh. Yousif, "Hybrid encryption using playfair and RSA cryptosystems," IJNAA, vol. 12, no. 2, Jul. 2021, doi: 10.22075/ijnaa.2021.5379.

[14] N. N. H. Adenan, M. R. Kamel Ariffin, S. H. Sapar, A. H. Abd Ghafar, and M. A. Asbullah, "New Jochemsz–May Cryptanalytic Bound for RSA System Utilizing Common Modulus N = p2q," Mathematics, vol. 9, no. 4. MDPI AG, p. 340, Feb. 08, 2021. doi: 10.3390/math9040340.

[15] M. Song, Y. Sang, Y. Zeng, and S. Luo, "Blockchain-Based Secure Outsourcing of Polynomial Multiplication and Its Application in Fully Homomorphic Encryption," Security and Communication Networks, vol. 2021. Hindawi Limited, pp. 1–14, Jun. 24, 2021. doi: 10.1155/2021/9962575.

[16] K. Limniotis,Cryptography as the "Means to Protect Fundamental Human Rights. Cryptography" 5(4), 34; https://doi.org/10.3390/cryptography5040034 ,2021.

[17] J.-P. Thiers and J. Freudenberger, "Code-Based Cryptography With Generalized Concatenated Codes for Restricted Error Values," IEEE Open Journal of the Communications Society, vol. 3. Institute of Electrical and Electronics Engineers (IEEE), pp. 1528–1539, 2022. doi: 10.1109/ojcoms.2022.3206395.

[18] Chong, B.; Salam, I. Investigating "Deep Learning Approaches on the Security Analysis of Cryptographic Algorithms". Cryptography 5(4), 30; https://doi.org/10.3390/cryptography5040030, 2021.

[19] El-Attar, N.E.; El-Morshedy, D.S.; Awad, W.A. "A New Hybrid Automated Security Framework to Cloud Storage System". Cryptography 2021, 5,37. https://doi.org/10.3390/cryptography5040037 ,2021.

[20] Raghad K. Saliha. "Optimizing RSA cryptosystem using Hermite polynomials". Int. J. Nonlinear Anal. Appl. 13 1, 955-961 ISSN: 2008-6822 (electronic) http://dx.doi.org/10.22075/ijnaa.2022.5614,(2022)

[21] C. D. Reddy, L. Lopez, D. Ouyang, J. Y. Zou, and B. He, "Video-Based Deep Learning for Automated Assessment of Left Ventricular Ejection Fraction in Pediatric Patients," Journal of the American Society of Echocardiography, vol. 36, no. 5. Elsevier BV, pp. 482–489, May 2023. doi: 10.1016/j.echo.2023.01.015.

[22] https://assets-global.website-files.com/5fb24a974499e90dae242d98/620a6854ba6d09814cb7ad0e_Table.png

[23] https://developers.google.com/machine-learning/crash-course/classification/precision-and-recall.