ENHANCED DEEP LEARNING BASED CRYPTOGRAPHIC METHOD FOR TEXT ENCRYPTION

1 V.Jayabharathi, 2 Dr.S.Sukumaran
1 Ph.D Research Scholar, 2 Associate Professor
1 Erode Arts and Science College (Autonomous), Erode-638009, Tamilnadu, India
2 Erode Arts and Science College (Autonomous), Erode-638009, Tamilnadu, India
1 vjayabharathimca@gmail.com 2 prof_suumar@yahoo.com

ABSTRACT
Security in network communication is of the utmost importance. The two primary elements of cryptography are encryption and decryption, which allow for the transmission of private and secret information through an insecure network. Unauthenticated users must not have access to data in order for them to utilize it improperly. Data encryption technology is widely used to protect the confidentiality of text data in the network, but when users need to access the data, the layer of encryption becomes a barrier. Cryptography is used to prevent the plain text of a cipher from being decrypted without the accompanying key. If you utilize solid encryption, it is practically hard to crack the algorithm or the key using brute force. The suggested task Advanced LightGBM algorithm describes the symmetric and dissymmetric of SCDA dataset text document and to directly process decrypted text. This ability to directly extract in the decrypted state aids in protecting the confidential data into encrypted format transmitted over the computer network key size value. The suggested approach for message communication in this paper is utilized to handle a variety of message kinds, making it possible to exchange special characters and ASCII characters more securely and quickly.

Keywords:Cryptographic text Encryption, SCDA dataset, ECC, Logistic Regression, Advanced LightGBM.

I. INTRODUCTION

The application of cryptography in modern research has an impact on people's lives. All types of research should first proclaim the security of text data rather than attempting to solve the issue of efficient information mining. Since ancient times, secure communication has used cryptography. The fundamental goal of cryptography is to change messages into encrypted form so that only the sender and the recipient of the information can decrypt and read the messages. In today's digital world, where tons of gigabytes, coming from online transactions, constantly flow over the Internet, communication processes are now mostly carried out using computer systems like personal computers, laptops, tablets, smartphones, etc., information security has become a real necessity. The computer scientists are very motivated to defend information against evil people since technology advances quickly. The main goal of cryptography is to prevent unauthorized access to information by using sophisticated mathematics and logic to obliterate information (encryption), then recovering the creative text data (decryption).

The study of cryptography focuses on data protection and providing security against intruders. A significant portion of security depends on sophisticated techniques to produce injective pseudorandom mappings that allow for both encryption and decryption activities. The effectiveness of cryptographic algorithms frequently depends on making the algorithms available to the public so that the community can research them for flaws and potential attacks. When a vulnerability is found, the method can then be modified or protected. Knowing exactly how the algorithm operates is the most crucial supplemental factor that must not be ignored, or at the very least, being relevant enough that only one person can require access to that information generates expectation [1]. The machine learning community has generated a fresh wave of interest in the area with its cutting-edge research.

Deep learning, machine learning, and artificial intelligence all gain from neural networks' capacity to reproduce the workings of the human brain. Neural networks, also known as artificial neural networks (ANNs) or simulated neural networks (SNNs), are the foundation of deep learning techniques. Their name and structure are also derived from the human brain since they mimic how actual neurons communicate with one another. Artificial Neural Networks (ANNs), which are information processing paradigms inspired by biological nervous systems like the brain, are shown in Fig. 1.1. The design of the information distribution system is a crucial element of this paradigm. It is composed of a huge number of intricately coupled processing units (known as neurons) that work together to solve certain challenges.Artificial neural networks (ANNs) learn by

imitating other things, just like humans do. An ANN is modified using a learning technique for a particular application, like text data categorization or pattern recognition [8]. One of the most sophisticated neural networks for supervised learning is this one. The network's structure consists of multilayer feed forward neural networks.

On the other hand, while the majority of the writers are [10] composed far attention, effective copies that need to be placed in the appropriate framework to exhibition the issues that have been stated as well as the difficulties that still remain. The goal of cryptography is to provide context for current research on the relationship between machine learning and cryptography.

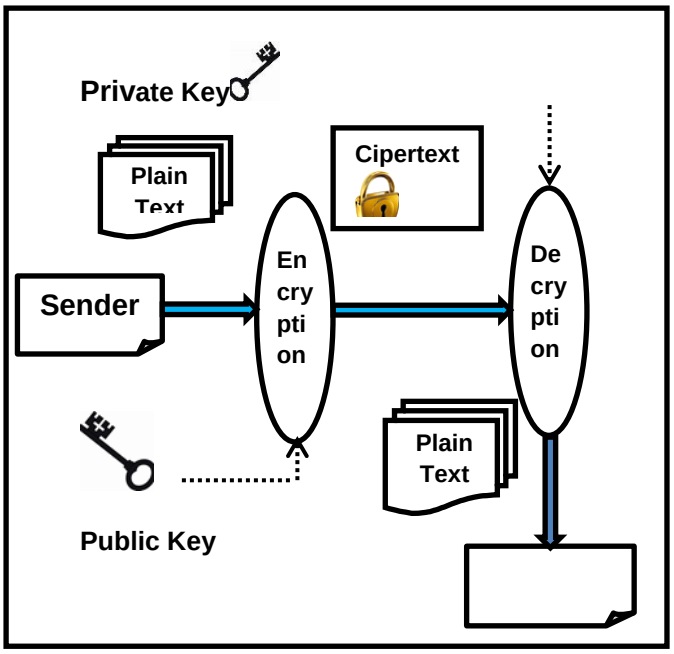

Fig.1.1 Text Encryption and Decryption

II. RELATED WORK

According to Kim et al. [11] in 2016, Bluetooth is a cheap short-range wireless communications medium. They suggested that the greater concern with these gadgets is security. They need a practical DES algorithm to make Bluetooth Technology useful for military applications.Bhardwaj et al.'s [2] 2011 work concentrated on using stream ciphers to encrypt data. Both base stations and mobile sites included the measured documents. The genetic algorithm is used to produce the keys. Utilizing single point approaches makes it easier to generate keys for encryption [7]. These natural algorithm strategies take into account multiple point crossover and variable population sizes as well as iteration counts. The goal of encryption is to convert plain text into cipher text. Applications for cryptography have created cipher algorithms that can be used to encrypt and decrypt ciphered images. Finally, using MATLAB control process, it was possible to depict the encryption and unscrambling of the images in the context of the RGB pixel and calculation.

Devin Reich et al. [5] proposed the text encryption approach as an effective information security measure in 2019. The equivalents of satisfied watermarking, content encryption, and a computation of content encryption with a view to common vernacular supervision are suggested. Three semantic modifications to everyday dialect preparation are discussed.

Key management, group interaction, and discussion based on generally trained neural networks have all been researched by SadeghRiazi et al. [13]. The synchronization of two parity machines, which are a sympathetic feed-forward neural network composed of one production neuron, K hidden neurons, and K*N input neurons, is necessary for the operation of a neural key exchange mechanism.

It is suggested that neural networks can be used as a secure key exchange system, rendering to [3]. Dual equivalence devices in this attitude, one for each side of the sender and receiver, receive the identical input vector, create an output bit, and perform training based on the output bit. Two neural networks that have been silently trained appear to reach a synchronization stage in which their time-dependent synaptic weights are identical. Finally, the generated secret key over a public channel is utilized for both encryption and decryption of data using traditional techniques like AES.

III. PROPOSED METHODOLOGY

The best option is singularity in cryptanalysis and encryption. The open text is composed primarily of punctuation, numbers, and characters from the international alphabet. The open text and the cypher text are equivalent in composition. Numerology and/or characters from other alphabets are commonly used. The ease with which information may be transmitted across multiple media is the fundamental cause of this.

The current paper analyzes data encryption, which is a method of protecting data by encoding it so that only a different person who has the exact encryption key may decrypt it or get the data. When a person or organization enters decrypted data without authorization, it seems muddled and otherwise unintelligible. The process of changing data from an intelligible arrangement to a twisted piece of information is known as data encryption. It is considered the work to shield secret information from prying eyes while it is being transported. Text documents, files, messages, and other

forms of network communication can all benefit from encryption.The ultimate goal of cryptanalysis is to enable keyless decipherment of a communication that has been encoded. Symmetric and asymmetric techniques are the two main ones used in encryption. Both parties share the encryption and decryption keys in symmetric encryption. P stands for plain text, K for the sender's secret key used to create C methods for encrypted text, otherwise known as cypher text,

C= Encrypt (K,P) ……..(1)

After it has been generated, the cypher text can be communicated. Once obtained, the cypher text can be decrypted with the same encryption key to get back to the creative fundamental document as shown below.

(K,C) = Decrypt (P)...(2)

In asymmetric encryption, one key is used for encryption and the other for decryption. The length of a cryptographic key is frequently specified in bits. No matter which cryptographic algorithm permits the addition of extra bits to the key, every new key is a chance to increase security.One of the most intricate neural networks for supervised learning is this one. The topology of the network is a multilayer suckle-onward neural network. The length of a cryptographic key is frequently specified in bits. No matter which cryptographic algorithm permits the addition of extra bits to the key, every new key is a chance to increase security.

One of the most intricate neural networks for supervised learning is this one. The topology of the network is a multilayer suckle-onward neural network. Neural network-based encryption and decryption techniques have shown to be efficient. We used parameters from both modified neural networks to construct cryptographic keys. An adjustment method for multilayer neural networks was backpropagation.

3.1 Elliptic curve cryptography (ECC)

The current cryptography method Elliptic curve cryptography (ECC) is a growing and effective cryptographic approach that has a variety of applications, including sensor networks, network security, authentication, signature verification, and many internet of things (IOT) applications. ECC is a more secure, effective, and portable alternative to other community key cryptography. To convert input message to elliptic curve opinion, numerous strategies must continue to be thought out, however they are all lacking in security, scalability, and computing efficiency for large input sizes. A scalable and capable algorithm for computation is therefore absolutely necessary. There are three different algorithms for input message to elliptic curve point conversion which will reduce communication cost and computational cost of encryption and decryption [17]. The investigational consequence similarly displays that the planned algorithms provide and improved concert besides the greatest appropriate for great scope input text associated to some other remaining algorithms.

3.2 Logistic Regression

The traditional cryptography process is Logistic regression is a widespread linear regression analysis typical. It is actually a classification method and it is often utilized in machine learning methods to solve binary classification problems. This model assumes that the data obeys the Bernoulli scattering. Inexploiting the probability function, inclineorigin is utilized to resolve the strictures, subsequently to attain the determination of binary classification of the data [4]. The possibility of the input X be appropriate to the first group is documented as, commonlywhile the probability is greater than 0.5, the output result is judged as 1, otherwise it is 0. Established on the prevailingtext data, a regression for the possibility of things happening. The logistic regression model is humble to appliance, actualeffective, require too much calculation is not necessary. The calculation only has relation to the number of features during classification, which is convenient for utilize in big data scenarios. The output is the probability score of each sample, which can be easily classified. At the same time, the form of logistic regression is simple, the model is clear, the probability derivation behind it can byattitudeanalysis, in addition to the interpretability is very respectable.

Y PY X X Y ==∈≤≤(1|)(R,0 1) …….. (1)

The logistic regression model function form is where Z is a linear transformation, and the linear transformation can be closer to the predicted value of the true value Y after a certain transformation relationship. The alteration association now is in the sigmoid purpose.

T Y Z Z w X b wb R ==+∈σ ……. .(2)

Utilize the gradient descent method to find the weight w and the offset b when the cost function is minimized. The gradient, the slope of the existingopinion, requires the bearing of association. The gradient descent method is to find the leastassessment, so it changes in the undesirablecourse of the gradient. Update w and b to be close to the lowest point of the cost function J curve, where α is learning rate representing the affectingperioddistance, which can be adjusted according to the model to obtain the optimal result. Most of the cryptographic algorithm identification schemes present in the literature employ single-layer machine learning classifiers. Complement Naive Bayes

was utilized. Conversely, single-layer classifiers may present low accuracies, over fitting and difficulties to find adequate parameters. In order to minimize possible problems that may exist in single-layer classifiers, this research evaluated the development of the classifier founded on collaborativeknowledge, which was called hybrid Logistic regression and Random Forest algorithm (HLRNRF).

3.3Proposed Advanced LightGBM Algorithm

Advanced LightGBM is a text encryption and decryption technology used for secure communication. In order to tackle the issue that the GBDT method is unable to balance processing time and data size, encryption is a framework that implements the GBDT algorithm. Additionally, it enables productive parallel training. To fit the new decision tree, the approximate residual value of the present decision tree is taken from the negative gradient of the loss function. The histogram approach, which Advanced LightGBM uses, overcomes smaller memory previously having inferior text data splitting complexity. The histogram algorithm's overall impression is to translate continuous floating-point text data into bin data and manage the number of bucket bins required for each characteristic. Then divided them equally, update the sample data belonging to the bucket to the bin value, finally represent it with a histogram.Then they were equally divided, the sample data from the bucket was updated to the bin value, and lastly it was represented by a histogram.

After discretizing continuous floating-point features into k discrete values and creating a histogram with a width of k, Advanced LightGBM negotiates the training data to count the growing statistics of each discrete value in the histogram. It is only necessary to traverse while performing feature selection in order to identify the best segmentation point that will give the histogram's discrete value. The most obvious benefit of using the histogram approach is the reduction in memory usage, albeit the computational cost is also sharply concentrated.

The quantity of the key forms that specify, of the positive as well as negative classifications of the model, and determining each and every line of the were to correct and determining how many were correct can be used to define accuracy. Recall is the percentage that shows how many of the model's positive categorizations were correctly classified, while precision is the number that shows how many of the model's positive categorizations were accurate in the first place.

The Gradient Boosting Decision Tree (GBDT) architecture known as the Advanced Light Gradient Boosting Machine (LightGBM) was built using the gradient depends on one-side sampling (GOSS) and special feature bundling (EFB) decision tree algorithms. Advanced lightGBM has difficulties with precision and effectiveness.

The continuous features can be discretized by the Advanced LightGBM algorithm, only utilizes the first-order derivative information when optimizing the loss function, the result tree in GBDT can private be a regression tree as well as every tree of the algorithm learns the assumptions and residuals of all farmer trees.

Proposed Advanced lightGBMAlgorithm of Text Encryption and Decryption

	Input : Initially, the inputGenerate the ASCII value of the letter are stored in an array of characters
Step 1:	***Each character in the list is converted into its corresponding ASCII values and stored in Valorg***
Step 2:	***The variable offset O f f setvar is generated using N, the first value of the initial key, and the properties of the tree—R, NL, and NR***
	For each character in the list, the initial reflected value ValInitial re f for each character is calculated
Step 3:	***ValRe f = ValRe f + dynamic o f f set***
Step 4:	***Get the Valorg for each character***
Step 5:	***while all words in inputlist are not iterated, do***
	word = pop word from input list
	for each character in word do
Step 6:	***Get ValInitial re f character, Get Dynamic offset***
	Let X = ValInitial re f + O f f setvar + O f f setconst
	if X is greater than Lenmax
	ValRe f [(X mod Lenmax) + O f f setconst + Dynamic offset]
	Else
	ValRe f [X + Dynamic offset]
	end if
	end for
Step 7:	***append Charactervalue of ValRe f to EncryptedWord append word or EncryptedWord to EncryptedLis***
	end while
Step 8:	***Reverse the number to get the Cipher text i.e. the plain text or original text***

The current research has a relatively high level of practicality and prediction of text keysize, but the times

are changing, the faster the information processing speed gives the improved results, the complication of text information is moreover enhanced, especially the proliferation of some popular information, especially online information areavailable in a lot of dynamic information. While automatic text classification can successfullycategorizenovelevidence, it is appropriateon behalf ofpresently processing and organizing this hugequantity of online text information. However, people's demand on the accuracy of search is higher and higher, which urges us to strengthen the effective text classification in a restored text classification.

Data encryption technology is a kind of special information transformation technology for both sides of communication according to the arranged rules. Generally collected of plaintext, ciphertextalgorithm in addition to key. Through the specific information technology to process the data, improve the appreciativeeffort and ensure that the information can only be obtained by the users authorized with special processing rules and ensures the security of information.

Encryption technology can be simply divided into two sharedgroups, specifically symmetric encryption and asymmetric key encryption. Symmetric encryption is a relatively traditional and simple encryption type, which utilizes the same key when encrypting and decrypting data.

Using symmetric encryption technology, the security of text data isresolute by on the key, but the security of key management is not guaranteed, which makes this encryption method difficult to implement in a trendyrequest. The understandablealterationamong asymmetric key encryption in addition to symmetric encryption is that a set of public key and private key systems are utilized. Secure Equality is presented in the data pre-processing method define a DES is a block cipher as well as encrypts data in blocks of size of 64 bits each, resources 64 bits of plain text energy as the input to DES, it produces the 64 bits of ciphertext. The same algorithm and key are utilized for encryption and decryption, with scale values of 0-1 handling missing text values.

Neural Networks are analogues that represent the functioning of biological neurons in the human brain. The artificial neural network consists of three layers: an input layer, an output layer, and an optional layer. Neural Networks are fully connected graphs which associated each node with an input value and each edge through the weight, that are initially accidentalstandardsin addition toadd which is always set.The initial permutation (IP) occurs merely on one occasion besides it occurs earlier the first round. It proposes in whatever the method the inversion in IP must continue, as exposed.The exactitude of the classifier is the foremostassessmentstructure which is assumed.

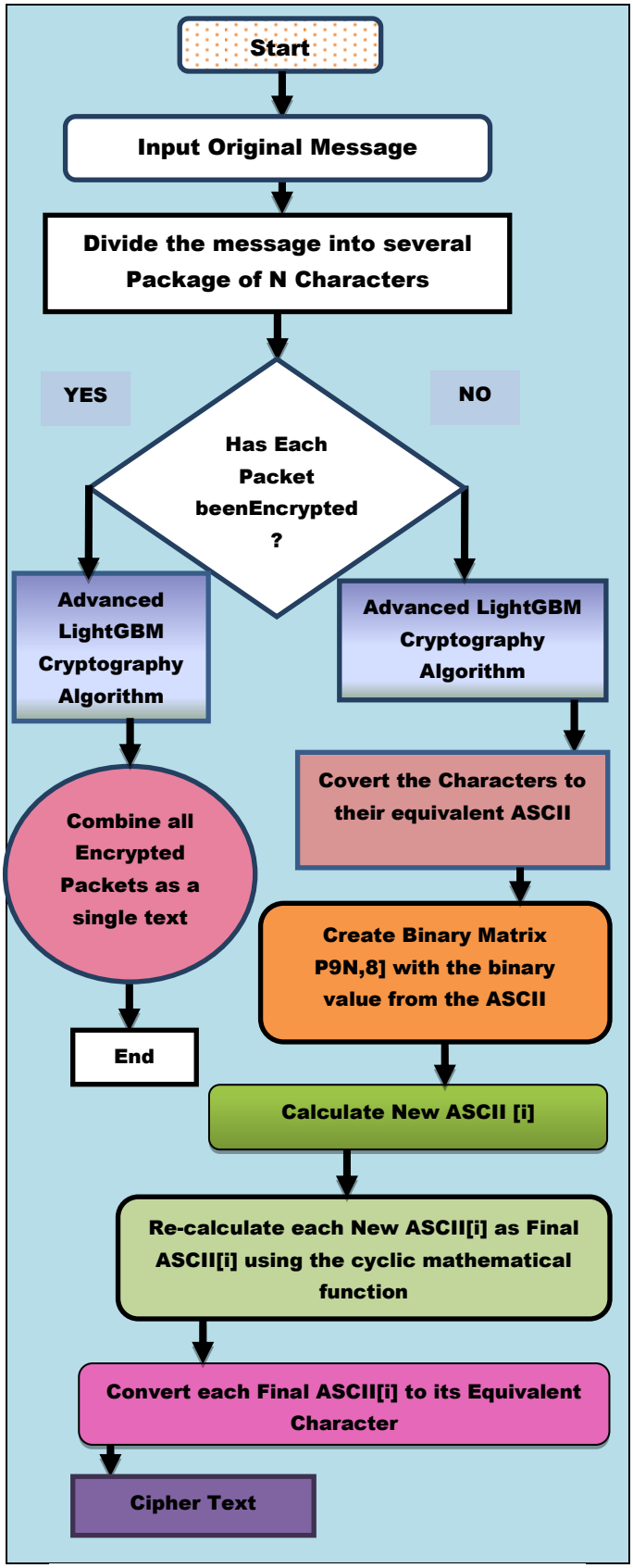

Fig.1.2 Flow Diagram of Advanced LightGBM Cryptography Algorithm

The first bit of the novel plain text block is replaced by the 58th bit of the original plain text, the second bit by the 50th bit of the novel basic text block, and so on.

• The Left Plain Text (LPT) and Right Plain Text (RPT) binary halves of the permuted block are created by the initial permutation (IP).

• At this point, the 16 rounds of encryption for each LPT and RPT are finished.

• As a Final Permutation (FP) is obtained on the collective block at the end, LPT and RPT are re-joined.

• 64-bit ciphertext is produced as a result of this process.

In order to evaluate the performance of the classifier, this research used accuracy as the primary criterion. Following an analysis of the results, it was determined that the Advanced lightGBM algorithm is the ideal configuration to encrypt confidential material and decrypt it in a convenient way.

A group of machine learning techniques called "Deep Learning" is based on artificial intelligence and uses numerous layers to gradually extract high-quality information. Deep learning is an effective learning technique that uses neural networks to carry out necessary tasks. The sigmoid function limits the standards to between 0 and 1 and has a superior S-shaped curve.

Sigmoid equals 1/(1+e-x).

The set of examples used to train the neural network in a deep learning model is known as the training dataset. The training accuracy is determined by the ratio between the number of examples that were successfully categorised and the total number of examples used as training data. Decrypted text data is used in the Hyper Parameter Optimization of Advanced LightGBM of Model Training.

3.3.1 Convolutional Neural Networks – Long short Term Memory

The text encryption value is predicted by the Convolutional Neural Network long short term memory, which was built to process data utilizing many layers of arrays. The design of CNN, which is mostly employed for pattern recognition, is comparable to the connection structure of human cognitive ability. Objectively, just as the human brain has billions of neurons, CNNs must have neurons arranged precisely. Contrary to popular belief, a CNN's neurons are built to mimic those in the frontal lobe of the brain, which is in charge of processing visual stimuli. The study assures that the complete graphic field is contained while also avoiding the fragmentary image processing issues of the

conventional neural networks, which call for feeding images in lower quality chunks. In comparison to adult networks, CNNs offer enhanced presentation when ASCII inputs are used in addition to linguistic or auditory signal inputs. The input neurons in the neural network are linked to the synchronized deposits. Shared weights are the definition of the mapping of the input layer to the hidden layer.

The LSTM network is one of the recurrent neural network architectures designed to temporarily recall the past of positive values. It has three gates: an input gate to read in input, an output gate to write out output to successive layers, and a forget gate to decide whether to remember and hide data. A variety of characteristics offered by LSTM enable fine-grained control of memory. With the use of these features, we are able to control how the present input affects the development of new memories, how old memories affect the way that new memories are designed, and which memory elements are essential for creating outputs. Short messages and odd characters can be delivered securely using the advised method.

IV. RESULTS AND DISCUSSIONS

To achieve the necessary safety phases, current symmetric encryption methods rely on static keys and multi-round functions. The goal of the proposed work is to decrease resource and latency requirements without sacrificing security. Computers handle the largest majority of current cryptography, and they are particularly adept at working with integers.

Symmetric technique has emphasized on improving conventional method of encryption by using substitution cipher text. Replacement techniques have utilized alphabet for cipher text.

Table 1.1Performance Evaluation of Advanced LightGBM Method

Algorithms	Composite Theory Calculus	Key Length Metric	Time Granularity	Mean Time to Detect
Logistic Regression	**0.6**	**0.65**	**0.66**	**0.63**
ECC	**0.7**	**0.78**	**0.73**	**0.75**
Advanced Light GBM	**0.7**	**0.73**	**0.72**	**0.73**

By utilizing substitution cipher text, symmetric approach has placed an emphasis on upgrading the current encryption method. For encryption text, replacement methods have used the alphabet. The plain text is essentially translated into the corresponding ASCII code value for each alphabet in this symmetric algorithm. explains in depth a number of symmetric key methods before putting out a fresh one. In Table 1.1, the experimental findings are shown.

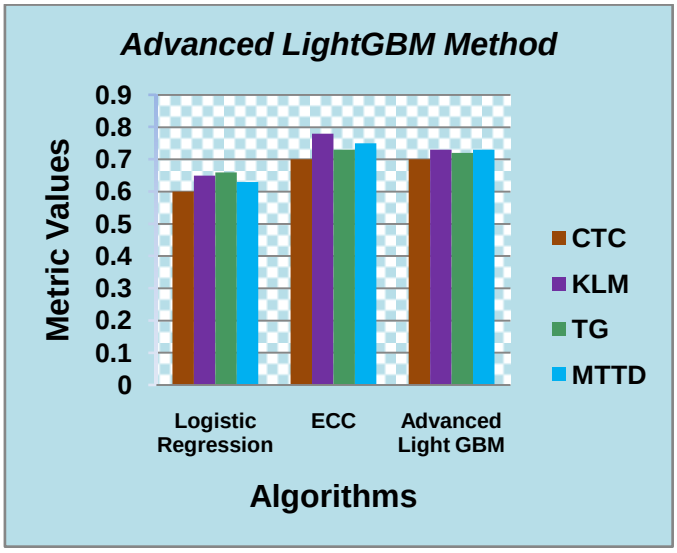

Fig 1.3Evaluation of Advanced LightGBM Method

Overall findings demonstrate the superiority of the Advanced LightGBM effect. A proposed metric for computing performance is CTC-Composite Theoretical Performance, which measures computing speed in millions of theoretical operations per second. It is assumed that the cryptographic algorithm being assessed or specified with this measure will only make use of computational primitive operations that are typically found on normal processors and primitives will be executed in operations.

The suggested Advanced LightGBM technique, shown in Fig. 1.3, uses a variety of cryptography-related metrics, including the KLM (Key Length Metric), which is a symmetric crypto system that operates as a function of length. The resistance to successful key length represented as a number of bits increases with key length. Too much consistency between TG- Time Granularity and the accuracy of the theoretical operation assumptions, it seemed. Mean Time to Detect, or MTTD, is an important component because it reduces the likelihood that an attack will do the least amount of damage possible given the encryption key size.

V. CONCLUSION

The suggested approach is utilized for message transactions and message-secured communication. It is possible to send special characters and messages of various types safely. The strategy is dependent on the message's character count, and straightforward calculations and operations are carried out to save execution time. Results of the proposed algorithm are compared to those of current algorithms for the metrics CTC, KLM, TG, and MTTD. The Advanced LightGBM is more efficient and helps to safeguard the secret data into an encrypted format with additional encryption processes.

REFERENCES

[1] Aono Y, Hayashi T, Wang L, et al. Privacy-preserving deep learning via additively homomorphicencryption[J]. IEEE Transactions on Information Forensics and Security, 2017, 13(5), Pp:1333-1345, Published Year 2017.

[2]Bhardwaj A, Subramanyam GV, Avasthi V, Sastry H. Review of solutions for securing end user data over cloud applications. International Journal of Advanced Computer Research. 2016; 6(27):222-9, Published Year 2016.

[3] Chialva D, Dooms A. Conditionals in homomorphic encryption and machine learning applications[J]. arXiv preprint arXiv:1810.12380, Published Year 2018.

[4] Conteh NY, Schmick PJ. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research. 2016; 6(23):31-8, Published Year 2016.

[5]Devin Reich, Ariel Todoki, Rafael Dowsley, Martine De Cock, and Anderson C. A. Nascimento. Privacy-Preserving Classification of Personal Text Messages with Secure Multi-Party Computation. In NeurIPS, Pp: 3752–3764, Published Year2019.

[6] Dodis, Yevgeniy, et al. "Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software." Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012.

[7] M. Hellman, "An overview of public key cryptography", IEEE CommunicationsMagazine, 2002, 40(5): Pp:42-49, Published Year 2002.

[8] Jacob, Theju, and Wesley Snyder. "Learning rule for associative memory in recurrent neural networks." Neural Networks (IJCNN), 2015 International Joint Conference on. IEEE,Published Year 2015.

[9] Kim A, Song Y, Kim M, et al. Logistic regression model training based on the approximate homomorphicencryption[J]. BMC medical genomics, 2018, 11(4): 83, Published Year 2018.

[10] Kumar B, Boaddh J, Mahawar L. A hybrid security approach based on AES and RSA for cloud data. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(17):43, Published Year 2016.

[11] Kumar B, Boaddh J. A meta-analysis on secure cloud computing. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(15):15, Published Year 2016.

[12] Rahul Chauhan, R.S.Joshi, "Convolutional Neural Network (CNN) for image Detection and Recognition", December 2018,DOI: 10.1109/ICSCCC.2018.8703316, Published Year 2018.

[13] Sun X, Zhang P, Liu J K, et al. Private machine learning classification based on fully homomorphic encryption[J]. IEEE Transactions on Emerging Topics in Computing,Published Year 2018.

[14] Shan W, Zhang S, He Y. Machine learning based side-channel-attack countermeasure with hamming-distance redistribution and its application on advanced encryption standard[J]. Electronics Letters, 2017, 53(14),Pp: 926-928, Published Year 2017.

[15] M. SadeghRiazi, Mohammad Samragh, Hao Chen, Kim Laine, Kristin E. Lauter, and FarinazKoushanfar. XONN: XNOR-based oblivious deep neural network inference. In Nadia Heninger and Patrick Traynor, editors, USENIX Security 2019: 28th USENIX Security Symposium, pages 1501–1518, Santa Clara, CA, USA, USENIX Association, Pp:14–16, Published Year 2019.

[16] M. SadeghRiazi, Christian Weinert, OleksandrTkachenko, Ebrahim M. Songhori, Thomas Schneider, and FarinazKoushanfar. Chameleon: A

Hybrid Secure Computation Framework for Machine Learning Applications. In AsiaCCS, Pp:707–721. ACM,Published Year 2018.

[17]Salomaa, Arto. Public-key cryptography. Springer Science & Business Media,Published Year 2013.
[18]Tanaka M. Learnable image encryption[C]//2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW). IEEE, Pp: 1-2, Published Year 2018.

Author profile

Dr.S.Sukumaran working as associate professor, Department of Computer Science (Aided) in Erode arts and science college,Erode,Tamilnadu,India. He is a member of board of studies in various autonomous colleges and universities. In his 33 years of teaching, he has supervised more than 55 M.Phil research works, guided 23 Ph.D research works, and still continuing. He has presented, published around 85 research papers in national, international conferences and peer Reviewed Journals. His area of research interest includes digital image processing, Networking, and data mining.

Mrs.V.Jayabharathi working as assistant professor , Department of Computer Applications in Sri Vasavi College,Erode, Tamilnadu,India.