FOREX Publication
Open Access | Rapid and quality publishing

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 2 | Pages 47-54 | ISSN XXXX-XXXX

Efficient Net B7 Convolutional Neural Network-Based Security and Privacy Preserving Method for Social IOT Environments

Maniveena. C[1] and Kalaiselvi. R[2]

[1]*Research Scholar, Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Thuckalay Kanyakumari, India, maniveena.cse@outlook.com*

[2]*Associate Professor, Department of Computer Science and Engineering, RMK College of Engineering and Technology, Puduvoyal, Gummidipoondi, Anna University, Chennai, India, kalaiselvi.rmk@outlook.com*

***Correspondence:** Maniveena. C; maniveena.cse@outlook.com

ABSTRACT- This year, one of the most widely used technical frameworks lacks a specific Internet of Things (IoT). Focusing on communication reliability and dependability on IPv6 standards and internet communication technology, the EfficientNet b7 Social IoT network satisfies care and adaptability needs. Despite the high-quality photographs this effort produced, there was some loss during the system's training, which takes time. This work suggested using evolution deep learning to automatically generate EfficientNet b7 feature frameworks for text classification tasks. The proposed approach is tested in the context of an EfficientNet b7-based language similarity analysis model to see if it works. While character-level EfficientNet b7 algorithms have not received much attention for text classification problems, the EfficientNet b7 structures proposed in this research have demonstrated exceptional performance in data classification tasks. A great deal of testing has shown that they are more resilient to disruptions and that they can impact numerous organizations that implement language and information usage policies regarding user privacy protection, framework implications, and legal requirements.

Keywords: Privacy Preserving, EfficientNet b7, Internet of Things, Security, Convolution neural network.

ARTICLE INFORMATION

Author(s): Maniveena. C and Kalaiselvi. R;

Received: 17/08/2023; **Accepted**: 25/09/2023; **Published**: 30/09/2023;
e-ISSN: XXXX-XXXX;
Paper Id: IJCSR-030106;
Citation: 10.37391/IJCSR.030106

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Traditional ones find it difficult to meet the increasing requirements of IoT-based UEs, including those related to Quality of Service (QoS). The Internet of cars, wearable technology, online gaming, and image authentication are just a few of the cutting-edge uses that have emerged lately and are catching on with customers. In the current digital era, the exponential expansion of Internet of Things (IoT) devices poses a variety of design difficulties for enterprises relating to security and privacy. According to previous studies [1], blockchain technology seems to be a substantial answer to the data security issues that the Internet of Things faces. Protecting privacy is growing crucial for contemporary cloud, Internet of Things (IoT), social media, and electronic health care applications. Images and medical information about patients are typically included in health and medical data, which should be kept private to protect patients' privacy [2]. Urbanization has made smart cities the norm thanks to the rise of the Internet of Things (IoT). Distributed smart devices can collect and process data inside the smart city's design thanks to Internet of Things (IoT) networks running on open channels via the Internet [3].

One of the main pillars of Industry 4.0, according to some, is the capability of Industrial IoTs, which has been made possible by efficient physical data sharing. Although these physical data are essential for many parts of a manufacturing system, they also raise serious privacy concerns for manufacturers and labourers, making data exchange more difficult [4]. Due in large part to the performance boost that cloud-based data management provides to IoT applications, with cloud assistance and technological movement, the IoT has gained traction. Using cryptographic techniques, data that is sent from IoT devices to the cloud is frequently encrypted. making it only decrypt able by a user chosen by the data owner [5]. Deep learning techniques have contributed significantly to the notable advancements in all fields in recent years [4-6]. An example of a deep learning network for computer vision that can recognise and classify picture features is the convolution neural network (CNN). EfficientNetB7, one of the CNN networks, continuously scales depth, width, and resolution while reducing the model size, yielding more effective results. Unlike other state-of-the-art CNN models that use ReLU as an activation function, EfficientNet uses a novel activation function termed Swish, which is a reduplication of linear and sigmoid activation functions. Thus, this methodology is used in the suggested research. The contribution of the paper:

- CNN's Social IoT network emphasizes the reliability of communication in relation to IPv6 protocols and

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 2 | Pages 47-54 | ISSN XXXX-XXXX

internet communication technology, which satisfies the needs for flexibility and care.
- The proposed approach is tested in the context of an EfficientNet b7-based language similarity analysis model to see if it works.
- Use two popular text classification datasets, one small and the other large, to assess the generalizability of the proposed application in a variety of text classification tasks.
- Compare the most improved classifiers to the most sophisticated EfficientNet b7 models that are currently on the market.

This is how the remainder of the paper is organized. Part II provides an overview of the related works. The suggested EfficientNet b7 for the techniques employed in this work is presented in Part III. Part IV results are discussed. Finally, Part V summarises the conclusion.

2. Related Work

Gheisari et al. (2021) [6] have detailed, high-level services require the sharing of data created by IoT devices with other parties. Automating municipal management is the goal of one of its products, Smart municipal. Our study presents a three-module design we term "Ontology-Based Privacy-Preserving" (OBPP) to address these issues.

To safeguard the confidentiality of the patient who is currently receiving treatment as well as the case database, Sun et al. (2021) [7] have investigated the secure recovery of patient records from past case databases. We create an ElGamal Blind Signature-based medical record search solution that protects privacy. A range of detection methods enabled by machine learning (ML) have been proposed by Cui et al. (2021) [8]. Due to its benefits of reduced latency and privacy preservation, recent efforts to improve detection performance have made use of federated learning (FL), a promising networked machine learning methodology.

Alzubi et al. (2021) [9] have described the BAISMDT paradigm aims to guarantee security and privacy in reliable data transmission for Internet of Things networks. For dependable and safe IoT data transfer, the suggested model uses signcryption. The process of securely transmitting medical data between IoT devices and service providers is facilitated by blockchain technology. In view of supplier rivalry and privacy issues, Xu et al. (2021) [10] have proposed using the reinforcement learning (RL) method to establish a privacy-preserving incentive structure for IoT devices and providers.

The study fills in the research gaps that were previously identified by Khaliq et al. (2022) [11], who suggested parking recommender systems that make use of elliptic curve cryptography (ECC) and local differential privacy (LDP). We suggested using a hash for a message authentication code (HMAC) mutual authentication scheme based on ECC that guarantees anonymity and communication integrity.

Shen et al. (2022) [12] have proposed federated learning mechanism, this work offers a privacy-preserving social computing framework for health management in order to address this difficulty. To minimize exposure, user data is stored on many user terminals. To address the mentioned issue, Shen et al. (2023) [13] have presented the We provide evolutionary privacy preservation learning techniques for an Internet of Things data sharing scheme based on edge computing. This approach involves applying evolutionary game theory and creating a reward matrix to precisely depict the interaction between edge nodes and Internet of Things devices, wherein they are considered as two sides in the game.

El-Haggar et al. (2023) [14] examined the Ubiquitous computing technologies (mobile, wireless, network) have given rise to the creative Ubiquitous Learning Environments (ULEs), which offer students learning opportunities outside of the conventional classroom, both in the real world and online. The enormous technological transformation brought about by ICT has given rise to a new technology called ubiquitous learning, or U-learning.

Kumar et al. (2023) [15] have described the single factor authentication has an impact on traditional IIoT user authentication procedures, making them less flexible as the number of users grows and diversifies into new user groups. This work attempts to use the developments in artificial intelligence techniques to construct the privacy preservation model in IIoT in order to address this issue.

Satyanarayana et al. (2023) [16] have described the task of routing in MANETs is not easy, and it has drawn a lot of interest from scholars worldwide. Through the augmented chaotic map, a new method is proposed for handling encryption and decryption procedures to handle MANET and IoT data. The SP-DAC method is a secure and private data categorization and aggregation solution, was suggested by Singh et al. (2023) [17] to utilize fog and cloud architecture. Using the SP-DAC approach, data is merged at the fog node and subsequently categorized by three machine learning models in the externalized cloud.

Shukla et al. (2024) [18] have described the IBOA is used in this case because it incorporates an extra-intense exploitation stage that directs the suggested framework to swiftly converge towards the global optimum while avoiding the trap of local optima. The CNN model for text similarity analysis is then integrated with the adversarial training idea.

Guda et al. (2024) [19] encrypts the data while providing fine-grained access control by utilizing the idea of ciphertext-policy attribute-based encryption (CP-ABE). The accuracy of the classifier, or Bayes Score, is calculated by estimating the joint probability of the data over multiple consumers.

Kumar et al. (2024) [20] have proposed masking sensitive and private information belonging to an individual using a deep neural network - statistical differential privacy (DNN-SPD) technique. The neural network's input layer receives input in the

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 2 | Pages 47-54 | ISSN XXXX-XXXX

form of both numerical and category-based human-specific data. In these methods the following disadvantages were found.

- Low accuracy with various methods for detection of text for real time image dataset.
- The methods can't detect all aspects in text, it effects on training.
- The existing methods can't detect new more features, it only collects unique features and detect as ensemble results.

The proposed method is designed to overcome these disadvantages.

3. Proposed Method

This section presents the CNN approach in the context of social IoT and gives a thorough explanation of our recommended security augmentation technique. The countermeasure samples are generated by our EfficientNetb7 technique. In this technique, we employ both the conflict samples and the original samples for training. We use adversarial training to improve the durability of our model. Here are some further details about the adversarial sample creation process and the framework building for semantic similarity analysis.

3.1. The attention mechanism-based adversarial convolution neural network model

Extraction of Mutual Information from Phrase Pairs: Position relations and relationships are always important factors that affect phrase semantics when analyzing similarity between sentence pairs. On the other hand, popular sentence pair similarity analysis methods consider the information that each phrase pair has in common. These semantic vectors are not sufficient to capture the complete information flow. This will seriously impair the accuracy of the model. The workings of attention are the foundation of our model. When the neural network gathers sentence information, its method will undoubtedly be far more accurate if the intricacies can be given more weight. Thus, the proposed framework computes the mutual data between the texts before feeding the pair into the anti-convolution neural network. Additional main themes include co-occurrence word position information embedding and word2vec word vector integration. Before features are retrieved, the word is first pre-processed. Preprocessing includes word cleaning, breaking, feature extraction, and identification. Initially, a significant quantity of noise data, such as misspelled words, words from other languages, and meaningless sentences, is usually included in training samples for information extraction. Such noisy data will have an effect on the fine-grained preference variables that were recovered.

Consequently, it is essential to denoise the evaluation data first. After that, splitting is eliminated to begin the feature extraction procedure, which will require more analysis. It entails removing affixes in order to get roots. For example, "cat" is the root that recognizes the strings "Cats," "cat-like," and "catty;" The word "stem" is the root of the terms "stemmed," "stemming," and "stemmed in conclusion, a portion of the speech-tagged function is employed to retrieve these speech segments from responses since nouns, verbs, and adjectives are more likely to convey fine-grained features.

$$w_2vembedding = \sum_i^n \sum_f^m cos(w_1, w_j) \quad (1)$$

The phrases "w_i" and "w_j" are used together. The matrix for word embedding for phrase pairing was determined using *equation (1)*. Next, the computation method given in *equation (2)*, is applied to obtain the weight matrix between phrase pairs. For every conceptual unit of a sentence, the row members of the matrix weight vector are added in relation to sentence B. Create a weight vector for each conceptual unit in relation to sentence A in sentence B by including the matrix column's constituents.

$$w2vmatrix = \sum_i^n \sum_f^m cos(w_1, w_j) \quad (2)$$

The number of words in a phrase affects its semantic alterations. and their relative placements in addition to the factors of context, text structure, and semantic similarity that Word2vec embedding considers. The process of position embedding results in an embedded weight matrix that is determined by the words' shortest path. Usually, retrieving the co-occurrence terms in the text is necessary before building the position integrated weight matrix. Next, a set of co-occurring words is created, with set comword = w_{c1}, w_{c2},... w_{ck}, set (A) (B), and k representing the quantity of press in the phrase. Get the word placements knowledge second.

3.2. EfficientNet b7 model

Despite the fact that many of the models are computationally demanding, their application in training the ImageNet dataset has expanded in complexity and success. One of the most advanced models, the EfficientNet model uses 66 M parameters to classify the ImageNet dataset with an accuracy rating of 84.4 percent, therefore it may be considered a set of CNN models. The eight models that make up the EfficientNet model range in size from B0 to B7; while accuracy increases greatly with the number of models, no discernible rise in the number of predicted parameters occurs. This novel activation function, called the Leaky ReLu activation function, is used by the EfficientNet in place of the Rectifier Linear Unit (ReLu). When breadth, resolution, and depth are consistently scaled at smaller model sizes, compared to other cutting-edge models, EfficientNet yields more efficient outputs. Using the compound scaling approach, establishing a grid to show how the baseline network's many scaling dimensions relate to one another is the first step when working with a fixed resource limitation.

Because of its greater "Floating point operations per second" (FLOPS) budget, EfficientNet was able to use the MBConv bottleneck, which was the primary building element introduced by MobileNet V2. MBConv employs direct connections between bottlenecks with substantially blocks have fewer channels than expansion layers because they consist of a layer that first expands before the channels are compressed. When the design's layers divide, the calculation is lowered by a factor of k2, where the 2D convolution window's height and width are

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 2 | Pages 47-54 | ISSN XXXX-XXXX

reflected by the kernel size, or k. Eq. (3), defines EfficientNet mathematically as:

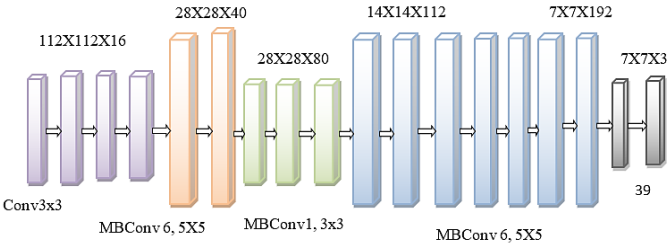

Figure 1. EfficientNetb7 architecture

$$p = \sum_{x=1,2,\ldots n} M_x^{Tx}\left(Y_{(A_x,B_x,D_x)}\right) \quad (3)$$

where Tx times are repeated in the variance of x, and Mx stands for the layer mean. With respect to layer x, the shape input in the tensor of Y is represented as (Ax, Bx, Dx). The data inputs are now 224X224 X3 instead of 256X256 X3. Increasing the accuracy of the model requires that the layers scale with a proportionate ratio optimized using the following formula:

$$max_{x,y,z} \quad Acc\big(p(x,y,z)\big) \quad (4)$$

$$p(x,y,z) = \sum_{s=1,2,\ldots n} M_s^{Ls}\left(Y_{(z.A_s,z.B_s,y.D_s)}\right) \quad (5)$$

Equation (4), uses x, y, and z to indicate the height, width, and resolution. *Equation (5)*, displays a number of the model's layers together with specific parameter information. *Figure 1*, shows a EfficientNet B7 architecture.

EfficientNet b7 Algorithm
Input: MSRP dataset
Output: classification
Train the CNN model using EfficientNet b7 architecture
Names =["block2","block4","block6","final layer"]
For name in name:do
Model_outer.layer[name]
End for
Output=output of final layer
Return output

3.3. The fundamental components of the Social Internet of Things

The SIoT architecture shown in *figure 2*, which is made up of six primary components: architecture, relation management, trust management, web services, information, and, lastly, SIoT tools, which comprise platforms and datasets.

The majority of papers suggested a four-tier design that consists of devices (objects), global connections, platforms, and applications based on IoT architecture, despite the fact that there is no standard architecture for SIoT. For devices to send or receive data from a specific platform or user application, they must be either directly or indirectly connected to the internet or a gateway. In order to read and exchange data between objects as middleware over the Internet, global connections are in charge of connecting objects to one another and acting as a communication layer between platforms and devices using communication standards, gateways, and protocols (MQTT, HTTP, HTTPS, and CoAP).

3.4. Security and Privacy

Non-Interactive Zero-Knowledge Arguments, A prover can persuade any verifier of a statement's validity using non-interactive zero-knowledge (NIZK) arguments without disclosing any more information. The most effective zk-SNARK technique, with a modest constant size and quick verification time, was put out by Groth [28]. We demonstrate arithmetic circuit satisfiability with committed inputs, parameters, and outputs through our work using a CaP Groth16 version.

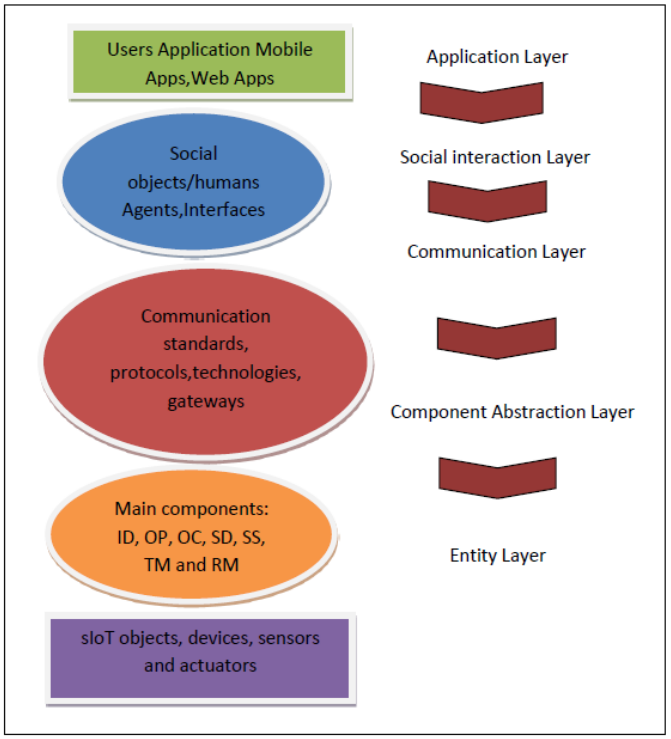

Figure 2. SIoT architecture

4. Experimental Results

4.1. Datasets

The MSRP (Microsoft Research Paraphrase Corpus) dataset is used in our investigation. The MSRP dataset was created using the Microsoft Research Semantic Corpus, which comprises 5100 pairs of English sentences from internet news sources. Python 3.7 is used in the implementation of the algorithm covered in this article. It contributes to the development of the DL model's framework. The Tensor Flow platform can also be used to build the anti-convolution neural network. Every task is completed using a computer system that has an Intel i5 quad-core CPU and 4 gigabytes of memory.

4.2. Performance Metrics

The proposed EfficientNet-B7 with convolution natural network (EfficientNetb7) model was assessed using a set of

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 2 | Pages 47-54 | ISSN XXXX-XXXX

MSRP data using performance metrics like confusion, area under the curve, specificity, precision, accuracy, and sensitivity, as well as F1-score. The accuracy of a sample's classification is displayed. The mathematical expressions for these measures are shown in *equation (6-9).*

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \quad (6)$$

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

$$sensitivity = \frac{TP}{TP+FN} \quad (8)$$

$$F1 - Score = 2\,x\,\frac{recall\ x\ precision}{recall+precision} \quad (9)$$

Accuracy is a metric for precise classification. This figure is important because it illustrates the frequency with which contaminated samples evade the model's identification. The provided models are assessed using performance metrics like the F1 score, specificity, sensitivity, precision, and accuracy. *Table 1*, show that the EfficientNetb7-biLSTM model has 94% accuracy.

Table 1. Comparative analysis of accuracy of different state-of-art methods

Model	Accuracy	Precision	Recall
DenseNet-201	92.8	99.5	91.5
ResNet-152	92.2	89.1	91.4
Firefly	71.3	90.4	91.2
EfficientNetsb7	94.01	99.7	92.9

The dataset was composed of 5100 data collection activities, which were divided into three groups: testing data (30%), training dataset (80%), and validation accuracy (30%). Only the training dataset was easily confused with the validating and testing datasets. With around 94.01% and 99.7% accuracy and precision, respectively, EfficientNetsb7 attained the highest levels. EfficientNetB7 shrinks the model and consistently scales depth, width, and resolution to give more effective results. Unlike other state-of-the-art CNN models that use ReLU as an activation function, EfficientNet uses a novel activation function termed Swish, which is a reduplication of linear and sigmoid activation functions.

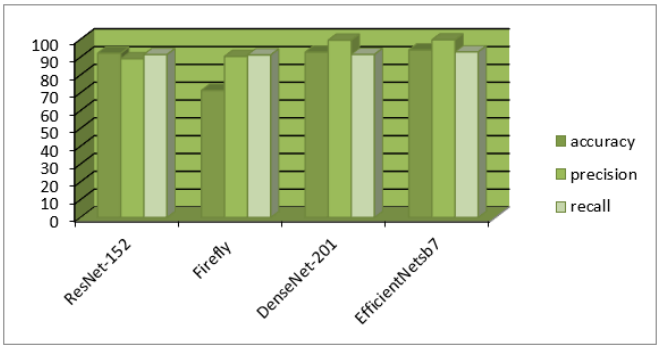

Figure 3. Comparison plot of proposed work with existing works

Additionally, with 92.9%, EfficientNetsb7 got the highest F1 scores. *Table 1*, and *figure 3*, demonstrate that the suggested system offers an accuracy rate of 99.7%, which is higher than other state-of-art approaches. When compared to other state-of-art techniques, the suggested EfficientNetsb7 employed produces better results.

The possibility that Internet of Things devices' queries may be rejected by edge nodes in this scenario is set at q = 0.8, whereas the odds that IoT devices will make malicious requests are set at p, 0.45, 0.47, and 0.49. Interestingly, it converges faster the lower the likelihood that harmful requests from IoT devices would occur, suggesting a higher likelihood of edge nodes complying with the requests. Using p = 0.45 and p = 0.49 as examples, it can be seen that whereas the latter needs the third game to decrease to zero, the former does so in roughly a half-game.

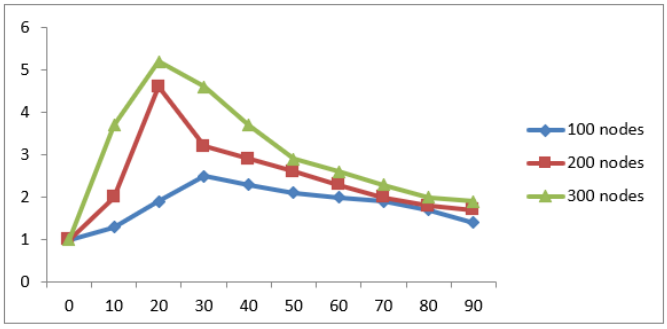

Figure 4. Edge node propagation shapes

If p is positive, then the transformation edge node approach which is depicted in *figure 4*, is assumed to be the approved request.

Shapes of edge node propagation: selecting a strategy when

$$p < \frac{\beta\gamma + \varepsilon}{2\pi\tau\epsilon - \alpha\delta\epsilon + \beta\gamma + \epsilon\rho}.$$

ROC curves

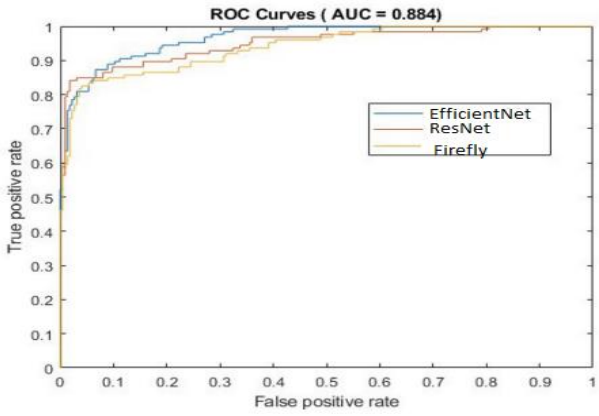

Figure 5. ROC curves of different methods

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 2 | Pages 47-54 | ISSN XXXX-XXXX

The area under the ROC curve (AUC) Ac, a useful metric for assessing how well a device can distinguish between two diagnostic classifications, is displayed in *figure 5*. The ROC curves derived with various deep learning techniques are displayed in *figure 5*.

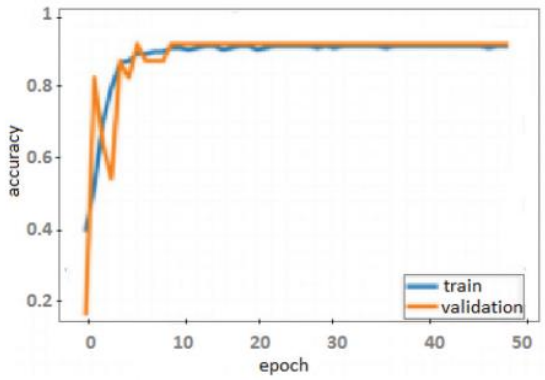

Figure 6. Accuracy vs. Epoch

The EfficientNetB7 method's region (Ac) under the ROC curve is larger than that of the other techniques, suggesting that it is closer to 1 than the others. Consequently, the recommended method has the highest capacity to discriminate.

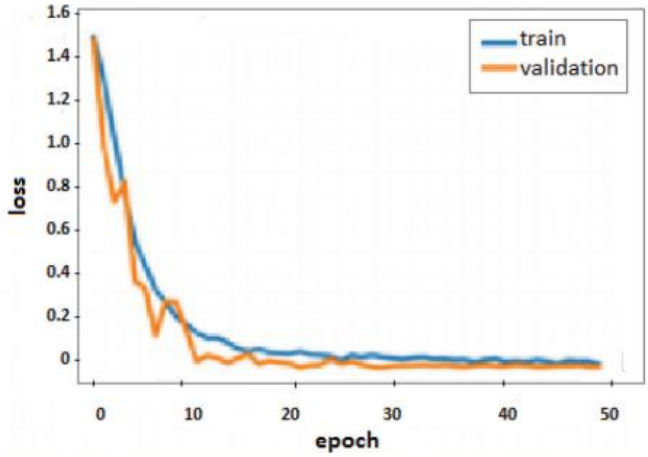

Figure 7. Accuracy vs. Epoch

Accuracy vs Epoch: The accuracy vs. epoch graph acquired during the training and validation phase is shown in Figure 6. It demonstrates the proposed system's great significance.

Loss vs Epoch: The suggested system is extremely significant, as demonstrated by the loss vs. epoch graph acquired during the training and validation phase, as shown in *figure 7*.

Friedman aligned ranking (FAR): We used the non-parametric Friedman aligned ranking (FAR) test to quantitatively confirm the superiority of the suggested approach. Table 2, lists and analyses the results of the FAR test using the area under the curve (AUC) measure. The following is the null hypothesis, or H0: All of the models are comparable, meaning that there isn't any major variation between them; on the other hand, the alternative hypothesis (H1) contradicts the first hypothesis. To determine the models' statistical significance, the Friedman test has been used in this instance. Based on their AUC, each model in the Friedman Test is given a rank. The lowest rank is given the greatest number, and the highest rank is given the smallest number. *Table 2*, demonstrates how effectively the suggested system outperformed the other available techniques, including Firefly and ResNet. A higher ranking (3.09) has been achieved by the suggested system.

Table 2. FAR rank based on the AUC curve

Methods	FAR rank
EfficientNet	3.09
ResNet	7.3
Firefly	9.5

Following the Holm procedure's rejection of the null hypothesis, the Post-Hoc test experiment was carried out. Using z-value and p-value, the Holm process calculates each model's performance in relation to the others. But after doing the Holm test, we got the outcomes that are displayed in *table 3*. *Table 3*, shows that for uncorrected p-values less than 0.001213, the hypothesis was rejected by the Holm test. Consequently, neither the suggested approach nor the KNN were disapproved. Conversely, only the ANN network was disqualified, exhibiting notable variations (poor performance) in contrast to the other techniques.

Table 3. Post-Hoc Holm test

Methods	Unadjusted p-value
EfficientNetB7	0.147299
ResNet	0.09769
Firefly	0.000084

5. CONCLUSIONS

This paper proposed to automatically create EfficientNet b7 feature frameworks for text classification tasks using evolution deep learning. This study suggests using the EfficientNetsb7 architecture to produce text with more distinctive features while lowering loss and training time. A novel adversarial text generation technique based on the EfficientNetsb7architecture is suggested. In addition, the concept of adversarial training is extended to the field of text similarity analysis with the proposal of an adversarial convolution neural network model. This research proposed an evolution deep learning strategy to automatically create feature EfficientNetsb7 frameworks for text classification problems. EfficientNetsb7 was able to create manufacturing method network topologies with only 25% of the datasets given. The recommended EfficientNetsb7 method performs better than other cutting-edge methods. In the third, we created a technical classification of the SIoT ecosystem's fundamental components. This classification comprises six subcategories: architecture, web service process, relation management, related information, trust management, or tools (platform and dataset). Each component is displayed individually to emphasise its advantages and disadvantages and convey its main concept. Furthermore, this research can be

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 2 | Pages 47-54 | ISSN XXXX-XXXX

developed and applied in further studies to evaluate the crucial components of SIoT, like friendship selection, relationship management, and trust management, more thoroughly and precisely. It might also investigate it for potential future research projects in interesting fields like smart cities, smart grids, and smart industries. We will continue to work on the numerous issues in this field that require in-depth investigation.

Author Contributions: The following statements should be used "Conceptualization, Maniveena. C and Kalaiselvi. R; methodology, Maniveena. C; software, Kalaiselvi. R; validation, Maniveena. C, and Kalaiselvi. R; formal analysis, Maniveena. C; investigation, Kalaiselvi. R; resources, Kalaiselvi. R; data curation, Maniveena. C; writing—original draft preparation, Maniveena. C; writing—review and editing, Maniveena. C; visualization, Kalaiselvi. R; supervision, Kalaiselvi. R; project administration, Maniveena. C; funding acquisition, Maniveena. C All authors have read and agreed to the published version of the manuscript".

Acknowledgments: The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

Conflicts of Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] Le Nguyen. B.; Lydia. E.L.; Elhoseny. M.; Pustokhina. I.; Pustokhin. D.A.; Selim. M.M.; Nguyen. G.N; Shankar. K. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. Computers, Materials & Continua 2020, Vol. 65, no. 1, pp.87-107.

[2] Hamza. R; Yan. Z; Muhammad. K.; Bellavista. P.; Titouna. F. A privacy-preserving cryptosystem for IoT E-healthcare. Information Sciences 2020, Vol. 527, pp. 493-510.

[3] Kumar. P.; Kumar. R.; Srivastava. G.; Gupta. G.P.; Tripathi. R.; Gadekallu. T.R.; Xiong. N.N. PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. IEEE Transactions on Network Science and Engineering 2021, Vol. 8, no. 3, pp. 2326-41.

[4] Zheng. X.; Cai. Z. Privacy-preserved data sharing towards multiple parties in industrial IoTs. IEEE Journal on Selected Areas in Communications 2020, Vol. 38, no. 5, pp. 968-79.

[5] Deng. H.; Qin. Z.; Sha. L.; Yin. H. A flexible privacy-preserving data sharing scheme in cloud-assisted IoT. IEEE Internet of Things Journal 2020, Vol. 7, no. 12, pp. 11601-11.

[6] Gheisari. M.; Najafabadi. H.E.; Alzubi. J.A.; Gao. J.; Wang. G.; Abbasi. A.A.; Castiglione. A. OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. Future Generation Computer Systems 2021, Vol. 123, pp. 1-3.

[7] Sun. Y.; Liu. J.; Yu. K.; Alazab. M.; Lin. K. PMRSS: privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare. IEEE Transactions on Industrial Informatics 2021, Vol. 18, no. 3, pp. 1981-90.

[8] Cui. L.; Qu. Y.; Xie. G.; Zeng. D.; Li. R., Shen. S.; Yu. S. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures. IEEE Transactions on Industrial Informatics 2021, Vol. 18, no. 5, pp. 3492-500.

[9] Alzubi. O.A.; Alzubi. J.A.; Shankar. K.; Gupta. D. Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things. Transactions on Emerging Telecommunications Technologies 2021, Vol. 32, no. 12, pp. e4360.

[10] Xu. H.; Qiu. X.; Zhang. W.; Liu. K.; Liu. S.; Chen. W. Privacy-preserving incentive mechanism for multi-leader multi-follower IoT-edge computing market: A reinforcement learning approach. Journal of Systems Architecture 2021, Vol. 114, pp. 101932.

[11] Khaliq. A.A.; Anjum. A.; Ajmal. A.B.; Webber. J.L.; Mehbodniya. A.; Khan. S. A secure and privacy preserved parking recommender system using elliptic curve cryptography and local differential privacy. IEEE Access 2022, Vol. 10, pp. 56410-26.

[12] Shen. Z.; Ding. F.; Yao. Y.; Bhardwaj. A.; Guo. Z.; Yu. K. A privacy-preserving social computing framework for health management using federated learning. IEEE Transactions on Computational Social Systems 2022.

[13] Shen. Y.; Shen. S.; Li. Q.; Zhou. H.; Wu. Z.; Qu. Y. Evolutionary privacy-preserving learning strategies for edge-based IoT data sharing schemes. Digital Communications and Networks 2023, Vol. 9, no. 4, pp. 906-19.

[14] El-Haggar. N.; Amouri. L.; Alsumayt. A.; Alghamedy. F.H.; Aljameel. S.S. The Effectiveness and Privacy Preservation of IoT on Ubiquitous Learning: Modern Learning Paradigm to Enhance Higher Education. Applied Sciences 2023, Vol. 13, no. 15, pp. 9003.

[15] Kumar. M.; Mukherjee. P.; Verma. S.; Kavita.; Shafi. J.; Wozniak. M.; Ijaz. M.F. A smart privacy preserving framework for industrial IoT using hybrid meta-heuristic algorithm. Scientific Reports 2023, Vol. 13, no. 1, pp. 5372.

[16] Satyanarayana. P.; Diwakar. G.; Subbayamma. B.V.; Kumar. N.P.; Arun. M.; Gopalakrishnan. S. Comparative analysis of new meta-heuristic-variants for privacy preservation in wireless mobile adhoc networks for IoT applications. Computer Communications 2023, Vol. 198, pp. 262-81.

[17] Singh. A.K.; Kumar. J. A secure and privacy-preserving data aggregation and classification model for smart grid. Multimedia Tools and Applications 2023, Vol. 82, no. 15, pp. :22997-3015.

[18] Shukla. P.K; Pandit. S.V; Gandhi. C.; Alrizq. M.; Alghamdi. A.; Shukla. P.K.; Venkatareddy. P.; Rizwan. A. Effective privacy preserving model based on adversarial CNN with IBOA in the social IoT systems for CEC. International Journal of Communication Systems 2024, pp. e5669.

[19] Guda. K.; Kavitha. K.; Sujatha. B. A Hybrid Multi-Client Filter Based Feature Clustering and Privacy Preserving Classification Framework on High Dimensional Databases. International Journal of Intelligent Systems and Applications in Engineering 2024, Vol. 12, no. 8s, pp. 93-107.

[20] Kumar. G.S.; Premalatha. K.; Maheshwari. G.U.; Kanna. P.R.; Vijaya. G.; Nivaashini. M. Differential privacy scheme using Laplace mechanism and statistical method computation in deep neural network for privacy preservation. Engineering Applications of Artificial Intelligence 2024, Vol. 128, pp. 107399.

[21] Tripathy. B.K.; Dutta. D.; Tazivazvino. C. On the research and development of social internet of things. Internet of Things (IoT) in 5G Mobile Technologies 2016, pp. 153-73.

[22] Ortiz. A.M.; Hussein. D..Park. S., Han. S.N., Crespi. N. The cluster between internet of things and social networks: Review and research challenges. IEEE internet of things journal 2014, Vol. 1, no. 3, pp. 206-15.

[23] Kim. J.E.; Fan. X.; Mosse. D. Empowering end users for social internet of things. InProceedings of the Second International Conference on Internet-of-Things Design and Implementation 2017, pp. 71-82.

[24] Atzori. L.; Iera. A. Morabito. G. Siot: Giving a social structure to the internet of things. IEEE communications letters 2011, Vol. 15, no. 11, pp. 1193-5.

[25] Gulati. N.; Kaur. P.D. When things become friends: a semantic perspective on the Social Internet of Things. InSmart Innovations in

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 2 | Pages 47-54 | ISSN XXXX-XXXX

Communication and Computational Sciences: Proceedings of ICSICCS 2017, Vol. 2, pp. 149-159.

[26] Gulati. N.; Kaur. P.D. Towards socially enabled internet of industrial things: architecture, semantic model and relationship management. Ad Hoc Networks 2019, Vol. 91, pp. 101869.

[27] Voutyras. O.; Bourelos. P.; Kyriazis. D.; Varvarigou. T. An architecture supporting knowledge flow in Social Internet of Things systems. In IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) 2014, pp. 100-105.

[28] Groth. J. On the size of pairing-based non-interactive arguments. InAdvances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques 2016, pp. 305-326.